

# PROTECTING AMERICANS FROM COVID-19 SCAMS

---

## HEARING

BEFORE THE

SUBCOMMITTEE ON MANUFACTURING, TRADE,  
AND CONSUMER PROTECTION

OF THE

COMMITTEE ON COMMERCE,  
SCIENCE, AND TRANSPORTATION  
UNITED STATES SENATE

ONE HUNDRED SIXTEENTH CONGRESS

SECOND SESSION

---

JULY 21, 2020

---

Printed for the use of the Committee on Commerce, Science, and Transportation



Available online: <http://www.govinfo.gov>

---

U.S. GOVERNMENT PUBLISHING OFFICE

52-684 PDF

WASHINGTON : 2023

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED SIXTEENTH CONGRESS

SECOND SESSION

ROGER WICKER, Mississippi, *Chairman*

JOHN THUNE, South Dakota	MARIA CANTWELL, Washington, <i>Ranking</i>
ROY BLUNT, Missouri	AMY KLOBUCHAR, Minnesota
TED CRUZ, Texas	RICHARD BLUMENTHAL, Connecticut
DEB FISCHER, Nebraska	BRIAN SCHATZ, Hawaii
JERRY MORAN, Kansas	EDWARD MARKEY, Massachusetts
DAN SULLIVAN, Alaska	TOM UDALL, New Mexico
CORY GARDNER, Colorado	GARY PETERS, Michigan
MARSHA BLACKBURN, Tennessee	TAMMY BALDWIN, Wisconsin
SHELLEY MOORE CAPITO, West Virginia	TAMMY DUCKWORTH, Illinois
MIKE LEE, Utah	JON TESTER, Montana
RON JOHNSON, Wisconsin	KYRSTEN SINEMA, Arizona
TODD YOUNG, Indiana	JACKY ROSEN, Nevada
RICK SCOTT, Florida	

NICK ROSSI, *Staff Director*

ADRIAN ARNAKIS, *Deputy Staff Director*

JASON VAN BEEK, *General Counsel*

KIM LIPSKY, *Democratic Staff Director*

CHRIS DAY, *Democratic Deputy Staff Director*

RENAE BLACK, *Senior Counsel*

---

SUBCOMMITTEE ON MANUFACTURING, TRADE,  
AND CONSUMER PROTECTION

JERRY MORAN, Kansas, <i>Chairman</i>	RICHARD BLUMENTHAL, Connecticut,
JOHN THUNE, South Dakota	<i>Ranking</i>
DEB FISCHER, Nebraska	AMY KLOBUCHAR, Minnesota
DAN SULLIVAN, Alaska	BRIAN SCHATZ, Hawaii
MARSHA BLACKBURN, Tennessee	EDWARD MARKEY, Massachusetts
SHELLEY MOORE CAPITO, West Virginia	TOM UDALL, New Mexico
MIKE LEE, Utah	TAMMY BALDWIN, Wisconsin
RON JOHNSON, Wisconsin	KYRSTEN SINEMA, Arizona
TODD YOUNG, Indiana	JACKY ROSEN, Nevada

## CONTENTS

---

Hearing held on July 21, 2020 .....	Page 1
Statement of Senator Moran .....	1
Prepared statement from Catherine Hermesen, Assistant Commissioner, Office of Criminal Investigations, Office of Regulatory Affairs, Food and Drug Administration, Department of Health and Human Services ..	3
Letter dated July 21, 2020 to Hon. Jerry Moran and Hon. Richard Blumenthal from Jonathan Spalter, President and Chief Executive Offi- cer, USTelecom .....	7
Statement of Senator Blumenthal .....	8
Statement of Senator Wicker .....	51
Statement of Senator Klobuchar .....	54
Statement of Senator Fischer .....	57
Statement of Senator Cantwell .....	59
Statement of Senator Capito .....	62
Statement of Senator Udall .....	64
Statement of Senator Baldwin .....	66
Statement of Senator Sinema .....	67
Statement of Senator Blackburn .....	69

### WITNESSES

Derek Schmidt, Attorney General, State of Kansas .....	9
Prepared statement .....	12
Andrew Smith, Director, Bureau of Consumer Protection, Federal Trade Com- mission .....	30
Prepared statement .....	31
Stu Sjouwerman, Founder and Chief Executive Officer, KnowBe4, Inc. ....	39
Prepared statement .....	41
Laura MacCleery, Policy Director, Center for Science in the Public Interest ....	42
Prepared statement .....	44

### APPENDIX

Response to written questions submitted to Derek Schmidt by:	
Hon. Jerry Moran .....	79
Hon. Dan Sullivan .....	80
Response to written questions submitted to Andrew Smith by:	
Hon. Jerry Moran .....	81
Hon. Marsha Blackburn .....	85
Hon. Dan Sullivan .....	86
Response to written questions submitted to Stu Sjouwerman by:	
Hon. Jerry Moran .....	87
Hon. Dan Sullivan .....	88
Response to written questions submitted to Laura MacCleery by:	
Hon. Jerry Moran .....	88
Hon. Dan Sullivan .....	91
Response to written questions submitted to the U.S. Food & Drug Adminis- tration by:	
Hon. Jerry Moran .....	91



## **PROTECTING AMERICANS FROM COVID-19 SCAMS**

---

**TUESDAY, JULY 21, 2020**

U.S. SENATE,  
SUBCOMMITTEE ON MANUFACTURING, TRADE, AND  
CONSUMER PROTECTION,  
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,  
*Washington, DC.*

The Subcommittee met, pursuant to notice, at 2:34 p.m., in room SD-G50, Dirksen Senate Office Building, Hon. Jerry Moran, presiding.

Present: Senators Moran [presiding], Thune, Fischer, Sullivan, Blackburn, Capito, Young, Blumenthal, Klobuchar, Udall, Baldwin, and Sinema.

Also present: Senator Wicker, Ex Officio, and Senator Cantwell, Ex Officio.

### **OPENING STATEMENT OF HON. JERRY MORAN, U.S. SENATOR FROM KANSAS**

Senator MORAN. Good afternoon. As Chairman of the Senate Commerce Subcommittee on Manufacturing, Trade, and Consumer Protection, I welcome you all here today to a hearing entitled, “Protecting Americans from COVID-19 Scams.”

The Nation continues to fight the unprecedented public health crisis brought on by the COVID-19 pandemic. In addition to the serious threat this pandemic poses to the health of Americans, the economic impact of the shuttered main-street businesses—resulting from responsible public health protocols have been felt in every corner of the country. It has become clear that preventive practices, policies, and dedicated resources, including expanding testing capabilities and the availability of personal protection equipment, are absolute necessities to a responsible path forward to reopening the economy and extinguishing this health crisis.

However, during this time of national emergency and coordinated recovery, there are fraudsters and scam artists that seek to take advantage of consumers, especially the Nation’s most vulnerable communities, like that of our Nation’s seniors. In fact, the FTC’s Consumer Sentinel Network reports that consumers across the U.S. have reported over 136,000 different cases of COVID-related scams, totaling approximately \$90 million in total fraud losses from January 1 to July 20, 2020. More specifically, at home in Kansas over this same period of time, consumers report over 500 related cases, totaling over \$800,000 in financial losses. Everyone should also bear in mind that these are the—are only the reported cases,

and that it is fair to assume that there are a number of harmful consumer scams that have not been reported to date.

The variety of these increasingly complex and innovative scams remains exceedingly difficult for any consumer to wrap their head around, much less defend themselves against. Whether it be unsubstantiated health benefits advertised for certain products, illegal robocalls pitching low-priced health insurance, fraudulent donation solicitations, or even imposters claiming to be from Federal agencies collecting mandatory payments, raising awareness to these harmful practices is critical to educating consumers and protecting themselves. As such, this subcommittee has much to learn from law enforcement agencies, industry, and consumer protection experts in their efforts to not only identify and address these harms, but also what exactly they are doing to prevent these harms from occurring in the first place. Additionally, if there is a role for Congress to play in supporting these efforts, those suggestions we will need today and in the future.

More specifically, I look forward to hearing from the Federal Trade Commission on how their current U.S. SAFE WEB authorities are utilized in addressing COVID-related scams stemming from abroad, and how enactment of the U.S. SAFE WEB Extension Act, which I introduced with the Ranking Member, Senator Blumenthal, is critical for continuing these foreign law-enforcement coordination efforts.

Additionally, I would be interested to hear from the witnesses about any specific efforts directed to particularly vulnerable groups of Americans, like our seniors. My colleague, Senator Klobuchar, joined me in introducing Protecting Seniors from Emergency Scam Act, which directs the FTC to report to Congress on scams testing—I'm sorry—targeting seniors during the—this pandemic, makes recommendations on how to prevent future scams during emergencies and, appropriately, to distribute such information to seniors and their caregivers.

Finally, the Subcommittee looks forward to hearing more about current enforcement efforts to detect, identify, and prosecute criminal organizations engaged in these illegal activities. If there are ways Congress can assist to strengthen the current framework of government task force—forces, join initiatives with State and local agencies and partnerships with the private sector to address the crimes, this subcommittee would, again, welcome the suggestions.

Today's witness panel provides a variety of different perspectives on the same important issue. Joining the Subcommittee is the Honorable Derek Schmidt, the Attorney General of the State of Kansas; Mr. Andrew Smith, Director of the FTC's Bureau of Consumer Protection; Mr. Stu Sjouwerman, Founder and CEO of KnowBe4, Inc.; and Ms. Laura MacCleery, Policy Director for the Center of Science in the Public Interest.

While the Food and Drug Administration was not able to join us today, the agency has been active in protecting consumers throughout this pandemic, and provided written testimony for the Subcommittee's consideration, and agreed to respond to questions for the record from the Committee members, as well.

[The information referred to follows:]

STATEMENT OF CATHERINE HERMSEN, ASSISTANT COMMISSIONER, OFFICE OF CRIMINAL INVESTIGATIONS, OFFICE OF REGULATORY AFFAIRS, FOOD AND DRUG ADMINISTRATION, DEPARTMENT OF HEALTH AND HUMAN SERVICES

### Introduction

Good morning, Chairman Moran, Ranking Member Blumenthal, and Members of the Subcommittee. I am Catherine Hermesen, and I serve as Assistant Commissioner of the Office of Criminal Investigations (OCI) within the Office of Regulatory Affairs (ORA) at the Food and Drug Administration (FDA or the Agency), which is part of the U.S. Department of Health and Human Services (HHS). Thank you for the opportunity to submit written testimony to discuss FDA's efforts to monitor and take action against firms that sell products with fraudulent claims of effectiveness against COVID-19.

I am pleased to submit testimony along with Mr. Andrew Smith, Director of the Bureau of Consumer Protection at the U.S. Federal Trade Commission (FTC), and the Attorney General of the State of Kansas, Mr. Derek Schmidt. FDA works collaboratively with FTC and our Federal and state law enforcement partners, as well as other Federal and state agencies, on a day-in and day-out basis across the Agency's programs, to ensure coordination across the Federal government and between the Federal government and the states.

FDA has a long history of investigating those who sell fraudulent products, which led to some of the Agency's, and its predecessors', founding legislation, such as the Pure Food and Drugs Act of 1906 and the Federal Food, Drug, and Cosmetic Act of 1938.<sup>1</sup> Our experience with previous outbreaks such as swine flu and avian influenza has shown that fraudulent cures or elixirs will emerge during any public health crisis, sold by unscrupulous actors capitalizing on the fears of vulnerable consumers. In 2003, FDA and FTC discovered several websites offering bogus Severe Acute Respiratory Syndrome (SARS) products, such as unapproved drugs offered for sale with claims to treat or cure the respiratory illness, as well as websites promising that consumers would be protected from SARS if they purchased and used items such as personal air purifiers, hand sanitizers, respirator masks, latex gloves, colloidal silver and oregano oil, and SARS "prevention kits" that packaged various items together, such as gloves and masks. Later, during the 2009 H1N1 influenza virus, FDA discovered online sales of counterfeit versions of the antiviral drug Tamiflu® (oseltamivir phosphate) shortly after FDA issued an Emergency Use Authorization during that public health emergency.

In the past months, we have seen an unprecedented proliferation of fraudulent products related to the COVID-19 pandemic, and more than ever before, the Internet is being used as the primary vehicle for marketing these unproven products. FDA considers the sale and promotion of these products to be a threat to the public health. Fraudulent COVID-19 products come in many forms, including medical devices like personal protective equipment (PPE) and diagnostic tests, purported vaccines, and even purported dietary supplements and other foods. Products like these that claim to diagnose, cure, mitigate, treat, or prevent COVID-19 and haven't been authorized, cleared, or approved for that use, not only defraud consumers of money—they also can place consumers at risk for serious and life-threatening harm. Using these products may lead to delays in getting proper diagnosis and treatment of COVID-19 and other potentially serious diseases and conditions; indeed, they may sometimes even cause serious illness or death themselves.

Fraudulent products have not been submitted to FDA for review, and may pose a serious safety risk to consumers. Beyond having no proven therapeutic value, these illegal products may contain dangerous substances or be adulterated with contamination and filth due to poor manufacturing standards. FDA oversight helps ensure U.S. consumers have access to safe and effective medical products. When fraudulent products attempt to bypass FDA and its scientific review, the results can be deadly.

### FDA's Long-Standing Collaboration with FTC

FDA and FTC have a long history of collaboration in protecting the health and wellbeing of the U.S. public, dating back to the 1920s. Between December 2002 and

<sup>1</sup> When the U.S. Department of Agriculture was created in 1862, the Patent Office's Agricultural Division was transferred to the new Department, becoming the Division of Chemistry in 1890 and the Bureau of Chemistry in 1901. In 1927, the Bureau of Chemistry became the United States Food, Drug and Insecticide Administration, and in 1930 the name was shortened to the U.S. Food and Drug Administration. Ten years later, in 1940, FDA was transferred from the U.S. Department of Agriculture to the newly created Federal Security Agency, which was renamed the Department of Health Education and Welfare in 1953, and again renamed the Department of Health and Human Services in 1979.

July 2003 alone, during the first SARS pandemic, the two agencies issued a combined total of more than 200 warning letters and other advisories to various companies selling unproven and fraudulent health products over the Internet and by other means. These requests for compliance were directed at several waves of fraudulent products offered for sale during that time period preying on consumers' fears about biological, chemical, and nuclear terrorism threats and the SARS epidemic. And in 2018, FDA and FTC issued joint warning letters to the sellers of unapproved opioid cessation products with false and misleading claims about their ability to help in the treatment of opioid addiction and withdrawal.

Most recently, in March 2020, FDA and FTC sent the first warning letters to seven firms that offered for sale unproven products—including teas, essential oils, and colloidal silver—with false and misleading claims to treat or prevent coronavirus, in violation of the Federal Food, Drug, and Cosmetic Act and the Federal Trade Commission Act.

#### **FDA's COVID-19 Fraud Task Force**

To address the rapid proliferation of fraudulent COVID-related products, earlier this year FDA quickly assembled a cross-agency task force. This task force combines FDA's scientific and regulatory knowledge of human and animal drugs, biologics, medical devices, and dietary supplements and other foods, with our investigators and special agents who specialize in health fraud, compliance and enforcement, cybercrime, and import operations, to issue warning letters and to employ the full complement of FDA's enforcement tools, including civil injunctions, debarments and criminal investigations.

At the outset, it became clear that the Internet was the primary mechanism for the sale of fraudulent COVID-19-related consumer products—creating an immediate problem: the speed at which sellers can post, change, move or remove listings for these products online. In fact, ORA investigators identified approximately 64,000 domain names registered from January–March 2020 that contained COVID-19-targeted terms—names like “covid19cure.com,” “coronavirus-home-kits.com” and “cureforcoronavirus.com.” Questionable social media and online marketplace postings were also widespread, and once the virus reached the U.S., FDA began receiving Internet-related complaints about, for example, fake COVID-19 cures, illegitimate test kits, and substandard or counterfeit respirators and face masks.

To proactively identify and neutralize these threats to consumers and the public health, in March 2020 FDA launched “Operation Quack Hack.” Operation Quack Hack leverages Agency expertise and advanced analytics to protect consumers from fraudulent products during the COVID-19 pandemic. Building upon our previous experience with illegal online pharmacies, a team of consumer safety officers, special agents and intelligence analysts triages incoming complaints about fraudulent and unproven medical products. Where appropriate, complaints are then sent to other agencies or to FDA Centers for additional review, or referred for a warning letter, civil action or criminal investigation. In some cases, following a preliminary investigation, the team sends an abuse complaint to the domain name registrars or online marketplaces. These abuse complaints are intended to notify companies that may not have been aware that their platforms were being used to sell an unapproved, unauthorized, or uncleared medical product during the COVID-19 pandemic.

Our task force has reported hundreds of online postings for fraudulent and unproven COVID-19 products, and has already contacted numerous parts of the online ecosystem to request that they be vigilant in removing unapproved, unauthorized, and uncleared products with false and misleading COVID-19 claims from their Internet sites. Nearly all of these listings were thereafter removed by the companies. In addition, the task force continues to monitor the Internet for new products, and to ensure that listings for fraudulent products that were previously removed by the online marketplaces, social media platforms, or domain name registrars do not return on new sites with the same or new fraudulent claims. The task force has identified several common products offered for sale with false and misleading claims to treat and prevent COVID-19, including colloidal silver, mineral solutions, and essential oils. And, for unapproved, unauthorized, and uncleared products coming from abroad, FDA screens imports to protect U.S. consumers. In addition, FDA has trained imports staff to screen products entering the U.S. using portable devices that improve detection of illicit products, increasing FDA's ability to prevent such products from being sold in the U.S.

We continue to monitor the online ecosystem for fraudulent products peddled by bad actors seeking to profit from this global pandemic, and will work with online marketplaces, domain name registrars, payment processors, and social media websites so that they can investigate and remove from their platforms products that

fraudulently claim to diagnose, cure, mitigate, treat or prevent COVID-19, and keep those products from reappearing under different names.

Of course, FDA also partners with other Federal regulatory and law enforcement agencies, including the FTC, and through the efforts of the U.S. Department of Justice (DOJ), to coordinate our investigations and enforcement activities and to efficiently collect and disseminate information related to surveillance findings, referrals, and consumer complaints about fraudulent and unproven products sold with claims to diagnose, cure, mitigate, treat, or prevent COVID-19 or coronavirus generally.

#### **Recent COVID-Related Enforcement Efforts**

As of July 1, FDA has reviewed thousands of websites, social media posts, and online marketplace listings, and we have identified more than 780 fraudulent or unproven products related to COVID-19 being offered for sale. These actions have resulted in issuing more than 80 warning letters to sellers of products like homeopathic drug products, nasal sprays, colloidal silver products, purported herbal products, chlorine dioxide products, antibody tests, and others to U.S. consumers. In addition, listings for more than 195 unapproved, uncleared, or unauthorized products that claimed to diagnose, cure, mitigate, treat, or prevent COVID-19 have been removed by online marketplaces, and the Agency has issued more than 260 abuse complaints to domain name registrars, resulting in those registrars taking 189 websites offline.

As noted above, FDA has a long-standing history of collaboration with the FTC, and we often coordinate activities related to companies marketing fraudulent COVID-related products. For example, in April 2020, FDA and FTC jointly issued a warning letter to a seller of fraudulent chlorine dioxide products, equivalent to industrial bleach, frequently referred to as “Miracle Mineral Solution” or “MMS,” as a treatment for COVID-19. FDA had received reports of people experiencing serious adverse events, including severe vomiting, severe diarrhea, life-threatening low blood pressure, and acute liver failure after drinking certain chlorine dioxide products. FDA had not approved the seller’s product for any use, despite the defendants’ claims that these products can be used to cure, mitigate, treat or prevent diseases such as COVID-19, Alzheimer’s, autism, brain cancer, multiple sclerosis and HIV/AIDS. Claims made on the seller’s websites, which provided a link to purchase MMS, included, “The Coronavirus is curable, you believe that? . . . MMS will kill it.”<sup>2</sup>

In response to the April 2020 joint FDA/FTC warning letter, the defendants indicated that they would continue to sell MMS in violation of the law; shortly thereafter, a Federal court issued a preliminary injunction requiring the seller to immediately stop distributing its unapproved and potentially dangerous product.<sup>3</sup> On July 9, 2020, the Court issued an order of permanent injunction against the entity defendant and two of the named individual defendants.<sup>4</sup> In a separate criminal proceeding, on July 8, the U.S. Attorney’s Office for the Southern District of Florida announced criminal charges against four defendants, resulting from a criminal investigation conducted by FDA’s Office of Criminal Investigations. The defendants were charged with conspiracy to defraud the United States, conspiracy to violate the Federal Food, Drug and Cosmetic Act, and criminal contempt.<sup>5</sup>

FDA also works with both U.S. and international law enforcement agencies to keep unproven products out of our country. For example, several months ago, we intercepted and investigated a case of misdeclared COVID-19 “treatment kits” offered for import. As a result, OCI special agents, with the help of domestic and international law enforcement counterparts in the United Kingdom, led the DOJ to bring a criminal complaint against a British man who sought to profit from this pandemic and jeopardize the public health.<sup>6</sup>

More recently, FDA has warned consumers and health care professionals about hand sanitizer products containing methanol, or wood alcohol—a substance often

<sup>2</sup> See: <https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/warning-letters/genesis-2-church-606459-04082020>

<sup>3</sup> See: <https://www.fda.gov/news-events/press-announcements/coronavirus-covid-19-update-federal-judge-enters-temporary-injunction-against-genesis-ii-church>

<sup>4</sup> See: <https://www.fda.gov/news-events/press-announcements/coronavirus-covid-19-update-daily-roundup-july-9-2020>

<sup>5</sup> See: <https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/press-releases/father-and-sons-charged-miami-federal-court-selling-toxic-bleach-fake-miracle-cure-covid-19-and>

<sup>6</sup> See: <https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/press-releases/uk-national-charged-shipping-mislabeled-and-unapproved-treatments-patients-suffering-covid-19>

used to create fuel and antifreeze that is not an acceptable active ingredient for hand sanitizer products, and that can be toxic when absorbed through the skin, as well as life-threatening when ingested.<sup>7</sup> We have seen an increase in hand sanitizer products that are labeled to contain ethanol but that have tested positive for methanol contamination. State officials have reported recent adverse events in both adults and children ingesting hand sanitizer products contaminated with methanol—including blindness, hospitalizations, and death. In addition to warning the public about these dangerous hand sanitizer products, we are communicating with manufacturers and distributors about recalling them. We continue to test hand sanitizers offered for sale to U.S. consumers, including those being offered for import into the country, and are maintaining and continually updating a list on our website of hand sanitizer products that FDA has recommended be recalled because they were tested and found to contain methanol or are purportedly made at the same facility as methanol-contaminated products.

COVID-related testing products have also been the subject of recent FDA action. Last month, FDA issued warning letters to six companies for marketing adulterated and misbranded COVID-19 antibody tests.<sup>8</sup> Violations outlined in the warning letters included: offering test kits for sale in the United States directly to consumers for at-home use without marketing approval, clearance, or authorization from FDA; misbranding products with labeling that falsely claims the products are “FDA approved”; and labeling that bears the FDA logo, which is not for use on private sector materials. At the present time, there are no diagnostic or antibody COVID-19 test kits that are authorized, cleared or approved to be used completely at home. Testing in the home can present unique and potentially serious public health risks, including whether a lay user can collect their specimen, run the test, and interpret their results accurately. While FDA has authorized several diagnostic COVID-19 tests for use with at-home collection of samples that can be sent to a lab for processing and test reporting, FDA has not authorized any serology tests for use with at-home sample collection. We have requested that the companies take immediate steps to correct the violations cited in the warning letters, including ceasing the sale of the products and preventing future sales.

### Conclusion

FDA will continue to collaborate with the FTC and our other Federal and state partners to protect consumers from fraudulent products peddled by bad actors seeking to profit from this global pandemic, and we strongly encourage anyone aware of suspected fraudulent medical products related to the COVID-19 public health emergency to report them to us. We are committed to protecting Americans from unsafe products, and will continue our efforts to find and stop those selling unproven products that fraudulently claim to diagnose, cure, mitigate, treat, or prevent COVID-19. Unscrupulous actors must not be permitted to take advantage of a pandemic to increase their profits while jeopardizing the public health.

FDA appreciates the support and interest of Congress, and this Subcommittee, in our work related to COVID-19. Thank you for the invitation to provide a written statement for the hearing.

Senator MORAN. Finally, USTelecom provided a letter for the record describing the collaborative efforts of companies in the Industry Traceback Group to actively trace and identify sources of illegal robocalls that have only increased in frequency during the pandemic.

I ask that this letter be submitted for the record.

Without objection, it is.

[The information referred to follows:]

<sup>7</sup> See: <https://www.fda.gov/drugs/drug-safety-and-availability/fda-updates-hand-sanitizers-methanol#products>

<sup>8</sup> See: <https://www.fda.gov/news-events/press-announcements/coronavirus-covid-19-update-fda-issues-warning-letters-companies-inappropriately-marketing-antibody>

Hon. JERRY MORAN,  
Chairman, Subcommittee on Manufacturing, Trade & Consumer Protection,  
Washington, DC.

Hon. RICHARD BLUMENTHAL,  
Ranking Member, Subcommittee on Manufacturing, Trade & Consumer Protection,  
Washington, DC.

Dear Chairman Moran and Ranking Member Blumenthal:

Thank you for holding today's important hearing examining the rise of scams occurring during the COVID-19 pandemic and strategies for Federal and state government and the private sector to work together to protect the public. In particular, I am pleased to share with the committee our work to combat illegal robocalls.

USTelecom leads the Industry Traceback Group, a SWAT team of providers across the wireline, wireless, VoIP and cable industries who collaborate to trace the source of illegal robocalls and coordinate with Federal and state enforcement agencies to bring these scammers to justice.

Unfortunately, robocall scammers were out in force during this public health emergency, using COVID-19 to trick, manipulate and otherwise prey on vulnerable consumers. As soon as these scams started appearing, we began to aggressively trace them around the world. We do not just go after the scammers, but the under the radar voice service providers who let billions of these junk calls onto our shared communications network in the first place. We then coordinate with industry to raise awareness about the source of the illegal calls and with enforcement officials at the state and Federal level.

Some of these tracebacks cut off paths into the United States for multiple COVID-19 robocalls scams. For example:

- The Industry Traceback Group traced a COVID-19 testing kit scam to a VoIP provider in the Philippines. ITG notified the provider it was carrying suspect traffic bound for the U.S. and within 24 hours the provider indicated it severed its relationship with the customer and the calls stopped.
- The Industry Traceback Group traced a COVID-19 HVAC duct cleaning scam to a Florida provider receiving the calls from Pakistan. After notification by ITG, downstream call providers receiving traffic from the Florida entity intervened and the calls stopped.
- The Industry Traceback group traced a COVID-19 work from home for Amazon scam. In about an hour, ITG traced the calls to a provider in California who stopped taking the illegal calls from a customer based in Utah.

The work of the ITG has been facilitated by the Senate's leadership in passing the TRACED Act, a landmark law that bolsters more government prosecution, including criminal prosecution of entities and individuals actively engaged in efforts to defraud Americans.

We are proud to coordinate and share information on illegal and often fraudulent robocalls with government partners, including the Federal Communications Commission, the Federal Trade Commission, the Department of Justice and virtually every state Attorney General. In separate letters in April and May related to our coordination to combat COVID-19 scams, the FCC and FTC called this public private partnership "essential to combatting the deluge of unlawful robocalls and protecting consumers and is particularly vital in swiftly identifying scammers who attempt to defraud consumers during the COVID-19 disease outbreak."

Thank you again for bringing added attention to this topic by holding today's hearing. USTelecom and the members of the Industry Traceback Group remain committed to working with Congress and across Federal and state enforcement agencies to combat illegal robocalls. More information about our work is available at <http://www.ustelecom.org/the-ustelecom-industry-traceback-group-itg>. We look forward to being a resource on this and other topics to you and your staff.

Sincerely,

JONATHAN SPALTER,  
*President and Chief Executive Officer.*

Cc: The Honorable Roger Wicker  
The Honorable Maria Cantwell

Senator MORAN. With that, I now turn to the Ranking Member, Senator Blumenthal, for his opening statement.

**STATEMENT OF HON. RICHARD BLUMENTHAL,  
U.S. SENATOR FROM CONNECTICUT**

Senator BLUMENTHAL. Thanks, Mr. Chairman. And thank you for having this hearing.

In the wake of almost every disaster in this country, no matter how dire, there are always bottom-feeders and con artists who exploit people's fears and hopes. We all know, probably everybody watching and listening today knows, there is no cure for COVID-19, and there is no vaccine or other medical prevention. That has not stopped the con artists and scams from exploiting people's fears and hopes. In fact, they have defied both science and common decency in taking advantage of people financially.

So, the scams range from invasion of privacy and products that are useless, price gouging, mortgage and student loan relief scams, false cures, and fake test cons. But, more than just financial loss, people face real healthcare danger. False cures can kill. False cures not only take people's money, they can kill. And deception can be deadly.

So, there are a variety of products. And, in fact, the FTC has issued 255 warning letters. Those 255 companies were defrauding and endangering consumers before they were caught. Those 255 companies are among hundreds of others that are still doing business. Those 255 companies have paid no cost—none—for breaking the law and harming people, despite the FTC's warning letters. And they are still doing business. They may have changed their marketing pitches to be slightly less deceptive and misleading, but they're still out there. And if warning letters will not protect consumers, we need stronger action.

On March 9, I wrote to the FTC and the FDA, calling on both agencies to take more aggressive action to stop the marketing and sale of fake coronavirus cures. Warning letters to marketers simply fail to give consumers fair notice, they fail to inform, they fail to correct wrong information, and they send no real signal to the market. There needs to be real deterrence, not just warning letters, a slap on the wrist.

I'm also alarmed that, again, we see high-tech firms enabling consumer harm through negligence and inaction. Last month, I wrote the FTC and the FDA on the dozens of unsafe supplements being sold on Amazon and other online marketplaces that claim to kill viruses. Amazon still has supplements, tonics, probiotics, in a search for the "COVID cure." We need to stop the snake-oil salesmen. I mentioned a number of my—of them in my March 9 letter; in particular, TV evangelist Jim Bakker, who recently promoted a celluloid silver on his show, claiming that it would eliminate viruses such as coronavirus. Another one, Cellular Silver, itself, claims to, quote, "achieve 99.99 percent complete kill against 660 microorganisms." Again, this is deception. We find these kinds of utterly false ads for Quinessence Aromatherapy, N-Energetics, GuruNanda, Vivify Holistic Clinic, Herbal Amy. There is a list, and it is growing.

So, many of us, I think, hoped that this crisis would pass swiftly and that we could return to a normal life, both the healthcare crisis and the economic crisis. We're 6 months into this pandemic. There's no end in sight to this horrendous national suffering. We've seen hardship and heartbreak. It has been aggravated, not reduced, by many of these false and misleading promises for products that threaten healthcare, endanger lives, take money from people unfairly and illegally, but also pose great dangers to public health. And if we can do something about them, Mr. Chairman, we will accomplish a lot of good for the American people.

Thank you.

Senator MORAN. Senator Blumenthal, thank you.

Senator MORAN. We now will hear testimony from our witnesses, and we will begin with the Honorable Derek Schmidt, Attorney General, State of Kansas.

**STATEMENT OF DEREK SCHMIDT, ATTORNEY GENERAL,  
STATE OF KANSAS**

Mr. SCHMIDT. Thank you, Mr. Chairman.

Chairman Moran, thank you for the invitation, and thank you for accommodating our remote testimony today. I'll admit it's the first time I've presented congressional testimony without leaving the Office of the Attorney General in Topeka, so we hope it lives up to your needs.

Mr. Chairman, you have—both you and the Ranking Member have laid out, I think very well, the framework in which we operate as a State-level enforcement agency. You have my written testimony. I certainly won't read it. I thought I would use my minutes here for oral presentation to just emphasize a few of the highlights that we've already presented to you in writing.

Let me first discuss one case, for the purpose of illustrating, not because that case is necessarily all that extraordinary, but it illustrates some of the types of enforcement actions that, at the State level, we are engaged in.

Now, I had already filed a lawsuit, prior to the COVID pandemic, against a defendant, a fellow named Shawn Parcels. I actually have both criminal and civil litigation pending against him and his related companies, so I'm obligated, at this point, to say that criminal charges, of course, are only accusations, and a defendant is presumed innocent unless and until proven guilty. But, on the civil side for the enforcement action, we had accused Mr. Parcels of violating our State's consumer laws by selling autopsy services, tissue recovery services, and other related types of services without having the qualifications to do so. We had him enjoined from operating within the State of Kansas. It was done by court order during the pendency of our litigation. And then along came COVID. And we received information, after the pandemic erupted into the public consciousness, that our enjoined defendant had set up some new companies and was peddling, essentially, the same services, although in a new package, outside of Kansas, beyond where he was enjoined; and specifically, he was marketing his unqualified services to families and individuals who were—had loved ones who were deceased as a result of COVID, to do autopsy and tissue recoveries, which—he is entirely unqualified. We were able to—be-

cause we have the case already pending, the investigation for the additional information didn't take terribly long. We were able to go back in front of our judge and receive an expanded temporary restraining order that prevents him from representing himself on any of this, including on the COVID-related services, and also bars him from leaving the State of Kansas without case-by-case permission from our court.

I use this case just to illustrate—you know, we often talk, at the broad policy level, about, sort of, the collective impact of cases and behaviors by groups of defendants, groups of companies, whatever it may be. And those are certainly important. But, at the end of the day, enforcement actions, at least at the State level, typically boil down to one defendant or an associated group of defendants, one group of victims, and one group of misconduct. And so, those are the types of cases we wind up dealing with, with some regularity.

Moving beyond that individual case, let me just mention some of the types of complaints of scams and related misconduct we've been receiving since the pandemic erupted on stage in March. We have investigations pending with respect to each of these categories. I won't be able to discuss the particular investigations, but I can certainly talk about the general approach and subject matter.

And let me say, as both you, Mr. Chairman, and the Ranking Member have already pointed out, the crooks and scam artists use the same tools they always use, in terms of trying to get into people's pocketbooks. They just change the messaging to reflect the current concerns about COVID and to prey upon what people are currently worried about.

So, we saw, for example—the first wave that we saw come in, that continues, were text-message scams related to contact tracing, something that, back in March, most Americans had never heard of. And the text messages would come in and claim along the lines of, you know, "This is an official communication letting you know that you've been in contact with a person who has tested positive for COVID-19. Please click on this link in order to get more public health information to help you know what you need to do next." Of course, it was a phishing e-mail. Clicking on the link resulted in an invitation to provide personal information that had nothing to do with any legitimate public health purpose. We put out a—an early consumer alert in our state on that to raise awareness and try to help people avoid the problem, because it's obviously much easier to prevent people from becoming a victim than it is to chase down their money once it's on, particularly when the scammers operate outside of our jurisdiction and often from offshore.

Another type of scam that we've seen a lot of complaints on, as already mentioned by Senator Blumenthal, are COVID prevention and treatment scams. It's everything you've read about, but they come in in all the usual ways, sometimes by robocall, sometimes by personal call, sometimes by text message, sometimes by e-mail.

We've seen PPE scams, claims to be able to sell PPE to folks, and then either there wasn't any PPE, or it existed but it was sub-par, or it existed and it was good, but it was stolen, it wasn't theirs to sell. We've seen all of the above.

We've seen scams related to stimulus checks, often government-impostor type of scam, communications saying to folks, "We're from the Small Business Administration, we're from the IRS, we're from a fill-in-the-blank government agency, and we're here to assist you in making sure you get the payment to which you're entitled."

And we've seen fraudulent unemployment claims. Usually the objective there is some—to get personal information and get a payment based on some type of identity theft.

Finally, Mr. Chairman, I might just say, from our standpoint, the ability to cooperate with Federal agencies is really critical. The vast majority of law enforcement in this country, especially on scams and frauds, is conducted at the State and local level. But, we are geographically and jurisdictionally limited, and it makes no sense for us to be doing our thing in the territory that is Kansas, and the Federal agencies to be doing their thing within the territory that is Kansas, and us not to be coordinating. So, we always coordinate very closely, particularly with our regional agency offices, usually out of Kansas City. We have very good working relationships with the principal agencies you'd expect for this type of work, whether it's HHS OIG, or the FBI, or the Secret Service, among others. And we have redoubled those efforts during COVID.

Two things I might suggest for consideration on a policy standpoint related to that. And I'll close with this, Mr. Chairman. One is, I do think there is room—and I've suggested this, I know, to you before COVID, and I think COVID has proven the point—I do think there is room for a more structured relationship between State-level enforcers—in our case, an Attorney General's office—and our regional Federal law enforcement partners. What I mean by that is, you know, the Federal agencies receive a lot of information. I get a lot of complaints directly from our citizens. They don't—sometimes citizens don't come to us, they go directly to a Federal agency. The Feds are limited, in terms of the size of scams and rip-offs they often will look at. They may or may not admit it, but the reality is, they have to make choices, and they naturally look at the larger cases. That's perfectly understandable. But, sometimes—and we've done this on occasion—it is very helpful if, when our Federal partners receive a complaint, and they've worked it up in part, because they're trying to figure out what they've got, and it turns out they've got a violation of law, but it's—it doesn't rise to the level for Federal prosecution or consideration. It is very helpful if they will then present it to us, as a prosecuting entity, and we can prosecute those cases under State law. Well, we've done that, particularly with HHS OIG, out of the regional office before, and it seemed—it makes us very happy, because it gives us more cases in our pipeline, and it seemed to make them very happy, I think because they have a place to send smaller cases that they've already invested time and effort in but don't rise to the level, routinely, of Federal prosecution.

And then the second and final thing I'd suggest for consideration, Mr. Chairman, there is one thing pending in the Senate that would be very helpful, I think, in advancing our capacity on some of this. It's Senate bill 2379. I know you're a cosponsor. I think others on the Subcommittee are, and we have talked about it. It's a measure that's been pending for several years now, and I'm hopeful that it's

got a path, perhaps as part of the next stimulus bill, if there is one. But, it would remove what I think is an arbitrary barrier in Federal law that currently prohibits states from using our Medicaid Fraud Control Units to detect, investigate, or prosecute Medicaid patient abuse, as opposed to systemic fraud—but patient abuse, unless that abuse occurs in an institutional setting. So, from a COVID standpoint, what that means is, if I’ve got somebody that we discover somehow is ripping off, is defrauding a Medicaid beneficiary in a home healthcare setting, trying to sell them, you know, bogus cures, or whatever it may be, for COVID, I currently am not allowed to use our Medicaid Fraud Control Unit assets, which are partially federally funded and, therefore, subject to Federal limitation, to investigate and prosecute that. I’ve got to find some other way to do it with some other resources. And I can’t figure out why that is, other than it’s a historical anomaly. And it would be very helpful if that limitation were lifted swiftly, because it would allow us to deploy already existing and in-place investigation and prosecution resources to address non-institutional COVID scams.

So, thank you, Mr. Chairman, for the opportunity to present the information.

[The prepared statement of Mr. Schmidt follows:]

PREPARED STATEMENT OF DEREK SCHMIDT, ATTORNEY GENERAL, STATE OF KANSAS

Chairman Moran, Ranking Minority Member Blumenthal, and Members of the Committee:

Thank you for the opportunity to present this testimony as the committee discusses the unfortunate reality that scam artists are exploiting this global pandemic in attempts to profit unlawfully. I appreciate the invitation to offer the perspective of a state attorney general’s office and share the types of scams that are being reported to our office, the ways our office is responding and the cooperative work we have engaged in with Federal partners.

#### **Expectations and Preparations**

While none of us has experienced a global pandemic on the scale of COVID-19, our office has had plenty of experience dealing with more localized disasters, such as tornadoes and floods. We know from that experience that scam artists often take advantage of those situations to prey on people during a time of distress and disruption. We expected COVID-19 would be no different. On March 12, our office issued the first consumer alert advising Kansans to keep up their guard and watch out for COVID-19-related scams, such as bogus products advertised as coronavirus prevention measures or treatments as well as bogus charities purporting to raise money for coronavirus research or to support coronavirus patients.

Later that same day, the governor of Kansas declared a state of emergency related to COVID-19, which triggered the Kansas price-gouging statute within the Kansas Consumer Protection Act. This statute prohibits “profiteer[ing] from a disaster” by forbidding suppliers from “unjustifiably increasing during a time of disaster the price at which any necessary property or service is offered for sale to consumers.” The statute prohibits increases of more than 25 percent in the price of necessary products compared with the business day before the disaster was declared, unless the supplier can show that the additional cost was justified such as by additional costs incurred by the supplier.

To respond to the expected influx of complaints regarding both COVID-19 scams and price gouging, we immediately created a new complaint form on our website specifically to report these activities. We also launched a temporary COVID-19 resources homepage, which contained a link to the complaint form and information related to our COVID-19 response, including the consumer alerts mentioned in my testimony. As our office moved to dispersed operations, we prioritized keeping our Consumer Protection Division functional to be able to timely respond to these complaints.

### **State v. Parcels**

The complaints we have received related to COVID-19 scams have resulted in numerous investigations, many of which remain underway. To date, the most significant enforcement action our office has taken was in relation to a case that was already pending against an individual who offered to provide private autopsies, tissue recovery and forensic services, although he was not a licensed physician or pathologist qualified under Kansas law to perform such services. We previously had sued this defendant for those sorts of activities not related to COVID-19 and he was under a temporary court order not to perform such services in Kansas while our lawsuit is pending. Once the pandemic began, we learned that the defendant had formed new businesses and websites, including social media, that offered consulting services for coronavirus and COVID-19. Specifically, he was offering to enter homes and businesses, perform swabs for purported coronavirus testing and examine deceased persons to determine if they were positive for COVID-19. The defendant was quoted in media reports stating he had contact with two families in New York for COVID-19 testing on deceased family.

In May, we sought and obtained from the judge in our pending lawsuit an amended temporary restraining order prohibiting the defendant from advertising, soliciting, accepting payment for, contracting, performing, or in any manner conducting business or consumer transactions in epidemiology and infectious disease, including coronavirus and COVID-19. In addition, he was prohibited from traveling outside of Kansas or the Kansas City metro area without the approval of the court.

The case, *State v. Parcels*, remains pending in Shawnee County District Court, Case No. 2019-CV-000233.

### **Contact Tracing**

Scams related to contact tracing were among the first to emerge. We received reports from local emergency management officials of text messages circulating claiming that “Someone who came in contact with you tested positive or has shown symptoms of COVID-19 and recommends you self-isolate/get tested.” The message then has a link to click for more information. The link went to a bogus website that collected personal information. Our office issued a consumer alert on this particular scam, warning Kansans that the text message was not legitimate and not to click on the link.

As part of a COVID-19 response bill passed by the Kansas Legislature and signed into law by the governor last month, we recommended inclusion of language to further protect Kansans from invasions of privacy through contact tracing. We are hopeful that in addition to protecting civil liberties, these restrictions in the state’s Contact Tracing Privacy Act will allow Kansans to more easily know when alleged contact tracing is in fact a scam, because it does not adhere to the requirements placed on legitimate contact tracers being employed by the state or a local health department.

The new legislation, which applies to both the state and to local government authorities, contains the following provisions to protect citizens’ civil liberties and the privacy of information collected through contact tracing:

- Participation in contact tracing must be voluntary. No person may be required to participate, nor forbidden from participating.
- Contact tracing may not collect information through cellphone tracking and may not use any information collected through cellphone tracking.
- Information collected through contact tracing must be used only for contact tracing, kept confidential and not disclosed. The information must be safely and securely destroyed when no longer needed for contact tracing.
- Only specified information may be collected by contact tracers. The list of information that may be collected must be established by the Secretary of Health and Environment through the open and transparent process of adopting formal rules and regulations.
- The government may not require any third party to collect contact data. Information voluntarily collected by third parties may only be obtained by the government with the consent of both the third party and the person the information relates to, or with a judicially supervised warrant.
- People working as contact tracers must receive training and must affirm that they are familiar with the privacy and civil liberties protections in the legislation.

We believe these were sensible solutions to put guardrails in place so Kansans would have the necessary confidence in contact tracing programs to be willing to participate voluntarily, knowing that their personal information would be protected.

We believe passage of this bill made Kansas the first state to pass COVID-specific protections on contact tracing, and we are aware that other states are currently considering similar legislation. I am also aware that both Chairman Moran and Ranking Member Blumenthal are interested in this topic and have introduced Federal legislation seeking to protect the privacy of information collected via contact tracing apps.

I have attached to my testimony an op-ed I wrote that was published by National Review Online regarding our contact tracing bill (Attachment 1), as well as an editorial from the Kansas City Star that called our bill a “pragmatic and deeply American approach.” (Attachment 2).

In a related action, a bipartisan group of state and territory attorneys general joined together in a letter to the chief executive officers of Apple and Google asking them to strengthen efforts to monitor the contact tracing apps available through their respective platforms and to remove those that are not associated with a lawful government purpose. A copy of our letter is attached. (Attachment 3).

### **Other Types of Scams**

In addition to the issues described above, our office has initiated a number of investigations related to scam reports we have received. While I cannot discuss these pending investigations in detail, let me describe common categories of scam reports that we have received:

- *COVID-19 prevention.* These scams involve the offering for sale of a product purported to help prevent the consumer from contracting COVID-19.
- *Personal protective equipment.* These scams involved the sale of masks purported to be N95 and other personal protective equipment. In some cases, these masks were not N95 and others involved the sale of PPE that we believe the supplier never possessed. Some legitimate merchandise offered in third-party marketplaces was likely stolen and diverted for resale.
- *Stimulus checks.* Following passage of the CARES Act, we suspected that the direct cash payments to individuals would spur scam artists, and issued another consumer alert. As expected, we received reports of Kansans who received text messages or e-mails offering assistance to the consumer to claim their stimulus payment.
- *Government imposters.* This always-popular scam reemerged with COVID-19 variations. We have reports of scam artists posing as the Small Business Administration offering assistance with SBA loan programs and Kansas Department of Labor officials offering assistance with unemployment benefits.
- *Fraudulent unemployment claims.* The unprecedented number of unemployment claims flooding our state system offered scammers using stolen identities the opportunity to file claims and receive the temporarily increased benefits.

### **Federal and Private Sector Cooperation**

Throughout the pandemic, we have been working closely with multiple Federal partners sharing information about scams that are being reported. Examples include:

- We have worked with the Food and Drug Administration on cases involving advertisement of COVID-19 prevention or treatment products.
- We are working with the Kansas Department of Labor, U.S. Department of Labor Office of Inspector General, Small Business Administration and the Secret Service on the government imposter scams and fraudulent unemployment filings.
- We have referred cases to several other Federal agencies, including the Federal Trade Commission, Federal Bureau of Investigation and the U.S. Attorney’s Office for the District of Kansas. The U.S. Attorney’s Office has also formed a COVID-19 Fraud Task Force, bringing together many of these agencies, including our office.

We have also worked closely with private-sector partners to combat fraud. The largest example of this has been working with the large online platforms for resellers—Amazon, eBay and Facebook Marketplace—to have listings taken down that were clear cases of price gouging or products that likely did not exist at all. For example, in three cases, consumers reported to us Facebook Marketplace ads showing toilet paper advertised for as much as \$11 per roll. In each case, we contacted Facebook and the listing was removed. In another case, eBay removed 57 listings and suspended sellers of N95 masks based on a complaint we provided.

### **Scams and Frauds that Victimize Medicaid patients—S. 2379**

We know the volume of COVID-19 related scams will stretch law enforcement resources at every level. One specific action we have advocated to make further resources promptly available is swift enactment as part of the COVID-19 response of S. 2379, which would repeal an outdated and seemingly arbitrary Federal statutory restriction on states' ability to use their Medicaid Fraud Control Units (MFCUs) to detect, investigate and prosecute abuse of Medicaid patients in non-institutional settings. The expanded jurisdiction would include financial abuses in the form of COVID-19 related scams and frauds targeting Medicaid beneficiaries who do not reside in institutions. Under current law, states have authority to use their MFCU assets to address fraud against the Medicaid program itself anywhere it may be found but may address the abuse of Medicaid patients—including financial abuse through COVID-19 scams—only if it occurs in an institutional setting.

With a growing number of Medicaid beneficiaries receiving services in home-care settings, and with the increasing isolation at home of many Americans, including Medicaid beneficiaries, because of COVID-19 related restrictions, eliminating this Federal restriction could immediately bring more enforcement resources to the fight. Attached is a bipartisan letter I sent, along with three other state attorneys general, supporting inclusion of this legislation in COVID-19 relief legislation (Attachment 4). It would be tremendously helpful if S. 2379 could become law soon.

### **Conclusion**

I sincerely appreciate the cooperative work being done at all levels to protect Kansans and all Americans from becoming scam victims during this time when we are already faced with challenges we have never before experienced. Thank you for conducting this hearing today to shine a light on the good work that is being done and to discuss ways that we can further improve our efforts.

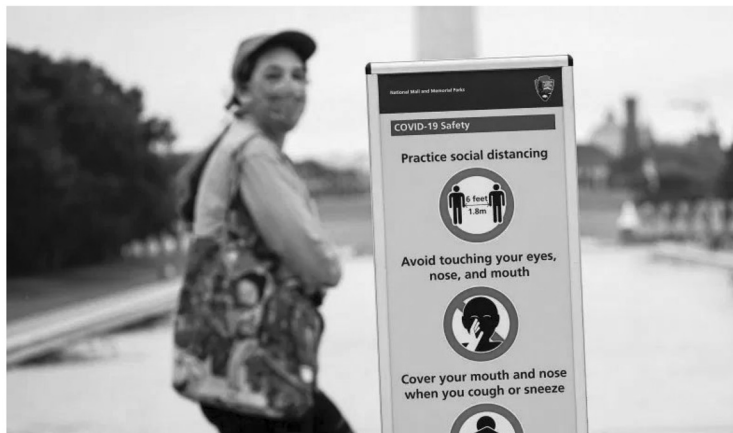
POLITICS &amp; POLICY

## How to Fight Coronavirus and Protect Civil Liberties

By DEREK SCHMIDT | June 18, 2020 6:30 AM



LISTEN TO THIS ARTICLE



A sign warns of coronavirus during Memorial Day weekend at the Lincoln Memorial in Washington, D.C., May 24, 2020. (Joshua Roberts/Reuters)

Our laws have not caught up with the scope and digital-age intrusiveness of COVID-19 contact tracing.

SINCE the plague ravaged Europe in the Middle Ages, fighting contagious and infectious disease has involved identifying those who come in close contact with

S infected persons, warning them of potential exposure, and advising they take precautions, such as monitoring for symptoms or self-isolation. To this day, many insist this process of “contact tracing” remains key to safely reopening America.

But COVID-19 is America’s first pandemic wholly of the digital age. When Swine flu began sweeping the globe a little over a decade ago, the iPhone was scarcely two years on the market and touch-screen Androids were unknown, the post-9/11 surveillance of Americans’ phone records was not yet revealed, and few had harnessed the tremendous power of personal data in marketing everything from consumer products to candidates.

Our thinking about the ancient practice of contact tracing needs to change with the times. Modern contact tracing presents more and different privacy and civil liberties concerns from, say, its pencil-and-paper ancestor during the 1918-19 Spanish Flu — and not only because of electronic tracking. Even data gathered the old-fashioned way by people making phone calls or knocking on doors to ask questions still present new digital-age challenges when compiled and potentially shared, manipulated, cross-referenced, and analyzed.

The scale of COVID-19 contact tracing further compounds each of these concerns. One report concluded that combating this virus may require 100,000 contact tracers to gather information about Americans’ health status, movements, and associations. Many thousands already are busily at work.

Despite this, the government’s use of contact tracing — and the personal information it gathers — remains largely unregulated. COVID-19 requires a new 21st-century mindset: How do we stop the spread of the disease *and* protect privacy and civil liberties?

Unfortunately, public health’s natural laser focus on stopping the virus can blind it to other legitimate concerns. For example, when I recently raised some of

these privacy and civil liberties issues in our state, a senior public-health official dismissively advised the public to “relax about that” and declared to our citizens that “I hope we won’t be muzzled by those who don’t share our concern for you.”

But concern for Americans’ well-being must include both our health *and* our liberties. Bland government assurances akin to “trust us, we’re here to help” provide little comfort.

All this understandably troubles many Americans. A survey released last month found that 84 percent were concerned about government misuse of personal information collected through contact tracing. Addressing those concerns is not only the right thing to do but also critical to obtaining sufficient public participation to contain the disease.

The root of the problem is that our laws have not caught up with the scope and digital-age intrusiveness of COVID-19 contact tracing. Few states have statutes regulating the practice. That changed recently in Kansas.

Earlier this month, the COVID-19 Contact Tracing Privacy Act was enacted with bipartisan support, placing Kansas at the vanguard in this area. I recommended our new law, which imposes important protections for civil liberties and privacy on both state and local governments, have the following provisions:

- Participation in contact tracing must be voluntary. No person may be required to participate, or prohibited from participating.
- Information may not be collected through cellphone tracking. While perhaps promising from a public-health standpoint, this seems to us disturbingly Orwellian and at least deserves pause for further study before government may undertake it.

- Collected information must be used only for contact tracing and kept strictly confidential and not disclosed. The information must be safely and securely destroyed when the task is finished. Bureaucratic mission creep is forbidden.
- Only specified information may be collected. Through an open and transparent process, the state health department must establish what may be gathered.
- The government may not use third parties to elude these protections. Government may not require businesses, for example, to collect contact-tracing information and may obtain voluntarily gathered information only with the consent of both the third party and the person the information pertains to, or with a judicially supervised warrant.
- People working as contact tracers must receive proper training and must affirm they are familiar with the law's privacy and civil-liberties protections.
- Contact tracers or governments are held accountable to these safeguards. Those who violate the Contact Tracing Privacy Act may face civil or criminal penalties, and any person may seek an injunction to enforce protections in the Act.

This legal framework is designed to protect privacy and civil liberties while public-health officials do their jobs. Rather than lecture and scold Kansans, our approach is to persuade, empower, and reassure. Kansans themselves bear the personal responsibility to choose our path forward by freely participating, or not, in ongoing efforts to track and contain the virus. We value both science *and* freedom, trusting in individuals more than government.



---

## Coronavirus Signs

Sign, sign, everywhere a sign ... A look at signs and billboards around the world informing people of coronavirus-related restrictions, social distancing requirements, and other measures meant to address the ongoing pandemic.

Pictured: A *Phantom of the Opera* sign asks people to wear a masks in public as the COVID-19 coronavirus outbreak continues in New York City, June 29, 2020.

Carlo Allegri/Reuters



---

*DEREK SCHMIDT is the attorney general of Kansas.*

## Attachment 2



**Worried about COVID-19 contact tracing and privacy - Kansas City Star, The (MO) - June 11, 2020**

June 11, 2020 | Kansas City Star, The (MO) | The Kansas City Star Editorial Board, The Kansas City Star

They tried mandatory contact tracing for coronavirus in one county in America — in Linn County, Kansas, just south of Kansas City — for all of two weeks. Epic fail. A losing proposition in both the courts and the court of public opinion.

Now, with a bill signed into law on Monday, Kansas is suddenly in the forefront of the nation in carefully regulated voluntary virus tracing.

That's huge. People need to be comfortable with contact tracing, which is as old as our knowledge of infectious disease. There is simply no way to reopen the economy safely, and for people to go back to work and school without fear or peril, other than minimizing the spread of COVID-19. The best way to do that is for all of us to get on board with contact tracing — not because the government says we have to, but because we want to stay safe and keep our neighbors safe.

Wisely, after the failed Linn County experiment in mandatory tracing, and following a script largely written by Attorney General Derek Schmidt's office, the Kansas Legislature and Gov. Laura Kelly agreed on a statewide contact-tracing regimen that is completely voluntary and unmenacing. Visitors and customers are not required, but are definitely strongly urged, to leave their contact information when they shop, eat and transact business. And businesses are implored to take it down so that cases of COVID-19 can be traced and those who are exposed contacted.

Interestingly enough, Schmidt believes a voluntary contact-tracing program is more likely to succeed than a mandatory one.

"There'd be a revolt if the government tried to really compel each person to do" contact tracing, Schmidt told The Star. "The way you get the participation is to assure people that they're not being ordered by the government to divulge this data, but they're doing it voluntarily for a good cause.

"I think the only way contact tracing can work is if it's voluntary. And I think the way you get people to participate in a voluntary system is to give them confidence that they can participate safely, securely and privately."

Thus, Kansas law requires contact-tracing information be limited, confidential, made available to the government only through agreement of all parties or through a judicial warrant, and destroyed when no longer needed. In addition, to make certain Kansas really has thought this through, the program expires a year from now, to ensure it's reviewed next legislative session.

That gives lawmakers added time to consider whether to also allow contact tracing via cellphone apps, which is expressly forbidden under the new law and frankly borders on Orwellian creepy.

It's a pragmatic and deeply American approach that we hope Kansans embrace. Schmidt says that in his office's research, it appears there are only one or two states that have anything close to Kansas' new citizen-centric structure for contact tracing. But expect other states to follow.

One key will be the contact tracers — the people who track down cases before they become outbreaks and warn those who've been exposed so they can take care of themselves and stay away from others. The Kansas Department of Health and Environment now has 300 contact tracing volunteers who are either being trained or who are awaiting assignment.

Thankfully, compliance with KDHE will be voluntary.

Linn County found out just how dicey mandatory contact tracing can be. One plaintiff in the lawsuit that brought down the mandatory tracing was a restaurateur who realized that some customers were refusing to dine out if their personal information was going to be forcibly handed over to the government.

Objection noted. With Kansas' new law making it voluntary statewide, there's nothing to fear from participating in contact tracing. The real fear needs to be transmission of the virus.

Voluntary contact tracing, as it turns out, may even be vastly superior to mandatory. But only if people pitch in and actually do it.

Copyright (c) 2020 The Kansas City Star



**PRESIDENT**  
Tim Fox  
*Montana Attorney General*

**PRESIDENT-ELECT**  
Karl A. Racine  
*District of Columbia Attorney General*

**VICE PRESIDENT**  
Tom Miller  
*Iowa Attorney General*

**IMMEDIATE PAST PRESIDENT**  
Jeff Landry  
*Louisiana Attorney General*

**EXECUTIVE DIRECTOR**  
Chris Toth

1850 M Street, NW  
Twelfth Floor  
Washington, DC 20036  
Phone: (202) 326-6000  
<https://www.naag.org/>

### Attachment 3

June 16, 2020

Mr. Sundar Pichai  
Chief Executive Officer  
Google, LLC  
1600 Amphitheatre Parkway  
Mountain View, CA 94043

Mr. Tim Cook  
Chief Executive Officer  
Apple, Inc.  
1 Apple Park Way  
Cupertino, CA 95014

Dear Mr. Pichai and Mr. Cook:

The undersigned Attorneys General ("State Attorneys General") write to express our strong concerns regarding the proliferation of contact tracing apps on your platforms that do not sufficiently protect consumers' personal information. Digital contact tracing may provide a valuable tool to understand the spread of COVID-19 and assist the public health response to the pandemic. However, such technology also poses a risk to consumers' personally identifiable information, including sensitive health information, that could continue long after the present public health emergency ends.

We are aware of your companies' joint development of application programming interfaces (APIs) that may be used to build decentralized exposure notification and contact tracing apps that utilize Bluetooth. Additionally, we understand from press reports and online materials that those APIs will only be available to public health authorities and that use of the APIs will be contingent on the inclusion of certain features to protect consumer privacy.

While we welcome your stated focus on a privacy-centered notification and tracing tool for future use, several COVID-19 related contact tracing apps are already available on Google Play and the App Store. Some of those apps may endanger consumers' personal information. We are particularly concerned about purportedly "free" apps that utilize GPS tracking, contain advertisements and/or in-app purchases, and are not affiliated with any public health authority or legitimate research institution.<sup>1</sup>

Moreover, as public health authorities release apps built with your APIs, there is likely to be increased media and consumer attention on exposure notification and contact tracing apps. Other developers may take advantage of the situation by placing new contact tracing apps on your platforms that do not adequately safeguard consumers' personal information

<sup>1</sup> For instance, as recently as early May, the first result when a consumer searches "contract tracing" on both platforms was an app called "Contact Tracing" developed by Piusworks, LLC, a California company with a suspended registration. According to the app information previously disclosed on Google Play, Contact Tracing uses geolocation tracking, contains ads, and offers in-app purchase, and it has been installed over 50,000 times. The app has since been removed from Google Play but is still available on the App Store.

in compliance with our states' laws. Therefore, we urge Google and Apple to take the following actions with respect to exposure notification and contact tracing apps available to U.S. consumers on Google Play and the App Store:

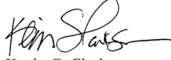
1. Verify that every app labeled or marketed as related to contact tracing, COVID-19 contact tracing, or coronavirus contact tracing or exposure notification is affiliated with a municipal, county, state or federal public health authority, or a hospital or university in the U.S. that is working with such public health authorities;
2. Remove any app that cannot be verified consistent with the above; and
3. Pledge to remove all COVID-19 / coronavirus related exposure notification and contact tracing apps, including those that utilize your new APIs, from Google Play and the App Store once the COVID-19 national emergency ends.<sup>2</sup> In addition, provide written confirmation to our offices that the apps have been removed or an explanation why removal of a particular app or apps would impair the public health authorities affiliated with each app.

Implementing these limited measures could help protect the personally identifiable information and sensitive health data of millions of consumers during this crisis.

Sincerely,



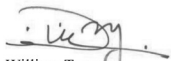
Douglas Peterson  
Nebraska Attorney General



Kevin G. Clarkson  
Alaska Attorney General



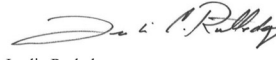
Xavier Becerra  
California Attorney General



William Tong  
Connecticut Attorney General



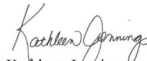
Ellen F. Rosenblum  
Oregon Attorney General



Leslie Rutledge  
Arkansas Attorney General



Phil Weiser  
Colorado Attorney General



Kathleen Jennings  
Delaware Attorney General

<sup>2</sup> This refers to the expiration of the emergency declared by the Secretary of Health and Human Services on January 31, 2020, under section 319 of the Public Health Service Act (42 U.S.C. 247d), and any renewals thereof.



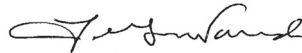
Karl A. Racine  
District of Columbia Attorney General



Leevin Taitano Camacho  
Guam Attorney General



Clare E. Connors  
Hawaii Attorney General



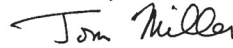
Lawrence Wasden  
Idaho Attorney General



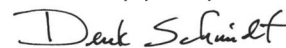
Kwame Raoul  
Illinois Attorney General



F. Aaron Negangard  
Indiana Chief Deputy Attorney General



Tom Miller  
Iowa Attorney General



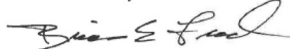
Derek Schmidt  
Kansas Attorney General



Jeff Landry  
Louisiana Attorney General



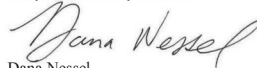
Aaron M. Frey  
Maine Attorney General



Brian Frosh  
Maryland Attorney General



Maura Healey  
Massachusetts Attorney General



Dana Nessel  
Michigan Attorney General



Keith Ellison  
Minnesota Attorney General



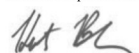
Aaron D. Ford  
Nevada Attorney General



Gordon MacDonald  
New Hampshire Attorney General



Gurbir S. Grewal  
New Jersey Attorney General



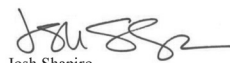
Hector Balderas  
New Mexico Attorney General



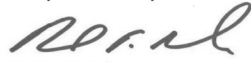
Josh Stein  
North Carolina Attorney General



Dave Yost  
Ohio Attorney General



Josh Shapiro  
Pennsylvania Attorney General



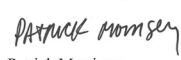
Peter F. Neronha  
Rhode Island Attorney General



Ken Paxton  
Texas Attorney General



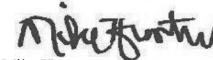
T.J. Donovan  
Vermont Attorney General



Patrick Morrisey  
West Virginia Attorney General



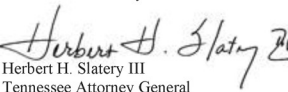
Wayne Stenehjem  
North Dakota Attorney General



Mike Hunter  
Oklahoma Attorney General



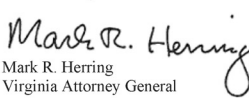
Dennise N. Longo Quiñones  
Puerto Rico Attorney General



Herbert H. Slatery III  
Tennessee Attorney General



Sean Reyes  
Utah Attorney General



Mark R. Herring  
Virginia Attorney General

## Attachment 4



STATE OF KANSAS  
OFFICE OF THE ATTORNEY GENERAL

DEREK SCHMIDT  
ATTORNEY GENERAL

MEMORIAL HALL  
120 SW 10TH AVE., 2ND FLOOR  
TOPEKA, KS 66612-1597  
(785) 296-2215 • FAX (785) 296-6296  
WWW.AG.KS.GOV

April 2, 2020

Honorable Mitch McConnell  
Senate Majority Leader  
317 Russell Senate Office Building  
Washington, DC 20510

Honorable Chuck Schumer  
Senate Minority Leader  
322 Hart Senate Office Building  
Washington, DC 20510

Honorable Chuck Grassley  
Chairman, Senate Finance Committee  
135 Hart Senate Office Building  
Washington, DC 20510

Honorable Ron Wyden  
Ranking Member, Senate Finance Committee  
221 Dirksen Senate Office Building  
Washington, DC 20510

**Re: Request for swift enactment of S. 2379 as part of national response to COVID-19**

Dear Leader McConnell, Leader Schumer, Chairman Grassley and Ranking Member Wyden:

As state attorneys general who manage our states' Medicaid Fraud Control Units (MFCU), we write to urge the Senate swiftly to pass S. 2379 as part of the national response to COVID-19. Current 'social distancing' and similar actions necessary to slow the spread of the virus are likely to increase social isolation of vulnerable populations, including Medicaid beneficiaries, who receive care at home or in other noninstitutional setting. That heightened isolation, in turn, increases the vulnerability of those individuals to abuse, neglect or exploitation. Enactment of S. 2379, which removes an arbitrary and unjustified statutory restriction on the use of MFCU assets to detect, investigate and prosecute the abuse of Medicaid patients in non-institutional settings can immediately bring to bear significantly more law-enforcement assets nationwide to combat this problem during this emergency.

The current federal, state and local emergencies in effect in response to COVID-19 present substantial challenges to the delivery of care to vulnerable populations in home health care and other noninstitutional settings. Prior academic literature has suggested emergencies could invite increased abuse, neglect and exploitation of isolated vulnerable populations such as elder persons or disabled persons.<sup>1</sup> One survey of

<sup>1</sup> See, e.g., Silvia Perel-Levin, *Abuse, Neglect and Violence against Older Persons*, UNDESA Expert Group Meeting on "Older Persons in Emergency Crises" (May 2019), available at <https://www.un.org/development/desa/dspd/wp-content/uploads/sites/22/2019/05/Silvia-Perel-Levin-Abuse-Neglect-and-Violence-against-Older-Persons-in-situations-of-emergencies.pdf> (last accessed March 26, 2020). See also Emily Ying Yang Chan, *Disaster Public Health and Older People* (Routledge 2020).

academic literature specifically identified financial abuse, neglect (primarily abandonment) and physical abuse (often domestic violence) of elder persons as particular concerns during disaster situations.<sup>2</sup>

In the current nationwide COVID-19 emergency, we are deeply concerned that one consequence is increasing social isolation of vulnerable populations, primarily elder or disabled persons, who live at home and in other noninstitutional settings. In ordinary times, these persons face heightened risks of abuse, neglect and exploitation because of their vulnerabilities. But during the current emergency, when social norms and service-delivery systems are disrupted, that risk is multiplied. As routine contact with these vulnerable persons is disrupted, we fear increased opportunity for abuse, neglect and exploitation to occur and go unnoticed. Consider the following:

- Ordinary social interactions that provide a sort of informal day-to-day oversight of these populations likely are suspended. For example, gatherings of “coffee groups” or “lunch groups” cannot occur because local restaurants may be closed or stay-home orders may be in effect.
- The ordinary structures of governmental oversight, such as interaction with Long-Term Care (LTC) ombudsmen, are interrupted. LTC ombudsmen typically do not go into home settings, but even in jurisdictions where LTC ombudsman home contact occurs it generally is being done only by telephone during the COVID-19 emergency. As a result, in-home visits that could notice irregularities that may indicate abuse, neglect or exploitation may not be occurring.
- The Adult Protective Services system is overtaxed and lacks sufficient personal safety equipment to safely enter homes during COVID-19.
- Many states have had to relax background checks on personal care attendants in order to recruit more persons into the field.
- Most states are now paying family members to care for loved ones. In the current situation, when no respite for family caregivers may be available because of the COVID-19 emergency, we fear a significant increase in violence. Sadly, family and other trusted caregivers often are the perpetrators of physical and financial exploitation.
- Meal delivery programs for vulnerable homebound persons may be interrupted during the current emergency, for example because of disrupted supplies, a lack of personnel, or other COVID-19 related reasons.

These are but some of the distressing circumstances arising from the COVID-19 emergency that present significantly increased risk of abuse, neglect or exploitation of vulnerable populations, including Medicaid patients who receive care in their homes or other noninstitutional settings.

Our MFCUs are powerful, existing law enforcement assets that are capable of responding to serious cases of abuse, neglect and exploitation of vulnerable persons. Indeed, they regularly do so when the abuse, neglect or exploitation occurs in a nursing home or other institutional setting. But current federal law prohibits the use of MFCUs to detect, investigate or prosecute Medicaid patient abuse that occurs in noninstitutional settings. S. 2379 would eliminate this arbitrary and unjustified restriction and enable us immediately to deploy existing MFCU assets to address reports of in-home abuse, neglect or exploitation of Medicaid patients during the current COVID-19 emergency.

<sup>2</sup> Gloria Gutman and Yongjie Yon, *Elder Abuse and Neglect in Disasters: Types, Prevalence and Research Gaps*, 10 Int'l J. of Disaster Risk Reduction, 38 (2014), abstract available at [https://www.researchgate.net/publication/263737165\\_Elder\\_Abuse\\_and\\_Neglect\\_in\\_Disasters\\_Types\\_Prevalence\\_and\\_Research\\_Gaps](https://www.researchgate.net/publication/263737165_Elder_Abuse_and_Neglect_in_Disasters_Types_Prevalence_and_Research_Gaps) (last accessed March 26, 2020).

Versions of this legislation have been thoroughly considered by Congress in recent years. Last fall, language identical to S. 2379 passed the House of Representatives 371 to 46 as part of bipartisan health-related legislation. S. 2379 now is pending in the Senate and has strong bipartisan support. This policy change has the support of the National Association of Attorneys General<sup>3</sup> and the Inspector General for the Department of Health and Human Services.<sup>4</sup> To the best of our knowledge, it is not controversial. And it can *immediately* make available existing MFCU assets to help protect the health and safety of many Medicaid patients who receive in-home services and who may, because of the extraordinary social disruption caused by the response to COVID-19, be at increased risk of abuse, neglect and exploitation.

But this important legislation can help protect vulnerable Americans during the current crisis only if it becomes law soon. We urge you to enact it swiftly as part of the Senate's coronavirus response.

Sincerely,



Derek Schmidt  
Kansas Attorney General



Lawrence Wasden  
Idaho Attorney General



Ellen F. Rosenblum  
Oregon Attorney General



T. J. Donovan  
Vermont Attorney General

Cc: Senator Marsha Blackburn  
Senator Mike Crapo  
Senator Ben Cardin  
Senator Maggie Hassan  
Senator Patrick Leahy  
Senator Jeff Merkley  
Senator Jerry Moran  
Senator Jim Risch  
Senator Pat Roberts  
Senator Bernie Sanders  
Senator John Thune

<sup>3</sup> On March 28, 2018, 49 state attorneys general sent a letter in support of the House version of this legislation, which was identical to S. 2379. A copy of that letter is available at <https://www.naag.org/assets/redesign/files/sign-on-letter/Final%20NAAG%20letter%20to%20Expand%20MFCU.pdf>.

<sup>4</sup> Testimony of Ann Maxwell, Assistant Inspector General, Office of Evaluation and Inspections, Office of Inspector General, Department of Health and Human Services, before United States House of Representatives Committee on Energy and Commerce: Subcommittee on Oversight and Investigations, at p. 10 (January 31, 2017), available at <https://oig.hhs.gov/testimony/docs/2017/maxwell-testimony01312017.pdf> (last accessed March 26, 2020).

Senator MORAN. General, thank you for your efforts, at our—in our home State, to protect consumers. Thanks for your testimony today. And thanks for your specific suggestions about Federal actions.

Now we turn to our next witness, Mr. Andrew Smith. He is the Director, Bureau of Consumer Protection at the Federal Trade Commission.

**STATEMENT OF ANDREW SMITH, DIRECTOR, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION**

Mr. SMITH. Thank you.

Chairman Moran, Ranking Member Blumenthal, and members of the Subcommittee, I'm Andrew Smith, the Director of the Federal Trade Commission's Bureau of Consumer Protection.

My written statement represents the views of the Commission, but this opening statement represents my views, alone, and not necessarily the views of the Commission or of any individual commissioner. I'm pleased to appear before you today to discuss protecting Americans from COVID-19 scams.

Despite the disruption of the coronavirus pandemic, the Bureau of Consumer Protection has managed to be aggressive, creative, and productive, particularly with respect to scams taking advantage of COVID-19 fear and confusion. Many of our specific initiatives of the last 4 months are outlined in my written testimony, but what is truly remarkable to me is how the entire Bureau of Consumer Protection has risen to the occasion and made a major contribution to the fight against COVID scams.

Each of our eight divisions and eight regional offices is pulling its weight in the fight against COVID scams while also keeping up with its existing load of projects and cases. Our Advertising Practices Division is taking action against fake cures. Our Marketing Practices Division is taking on robocalls and spurious business opportunities. Our Privacy Division is focused on videoconferencing, contact tracing, and issues around Ed Tech and distance learning. Our Financial Practices Division is fighting small-business financing fraud. Our Enforcement Division is taking on fulfillment scams that promise PPE to consumers but that never deliver. Our Consumer Response Division is collecting and analyzing complaint data for public consumption as well as improved law enforcement targeting. Our Litigation Support Division is assisting with innovative ways to continue to do our work remotely, including remote courtroom appearances, testimony, and document production. Our Division of Business and Consumer Education has produced dozens of blog posts, infographics, shareables, videos, and other material in five different languages, on the wide range of COVID scams, and has also been conducting extensive outreach directly and through our partners in the media, advocacy organizations, and trade groups. And our regional offices are doing all of the above, actively engaged in warning letters, investigations, litigation, and TROs. Outreach, outreach, and more outreach with State and regional partners.

In fact, just in the car on the way up here, I saw—I got a—an e-mail about a joint letter that our Chicago office had done with the Missouri Attorney General on a warning letter to two separate

companies, warning them against making fake claims for COVID relief in connection with hearing aids. Just within the last hour, we did that.

None of this, none of the work that we're doing, however, would be possible without the cooperation and coordination with our Federal, State, and local partners, as well as the private sector. Working with FDA, we've sent dozens of warning letters to dietary supplement sellers. We've been working with the Federal Communications Commission and the USTelecom Industry Traceback Group to halt illegal robocallers. Working with SBA, we've taken action against companies offering PPP financing to small businesses without SBA approval.

Some of our enforcement actions have been in conjunction with DOJ or other criminal authorities who execute search warrants at the same time as we go to court for an emergency TRO. State regulators and AGs are joining us in warning letters or taking action against recipients of our FTC warning letters. Foreign regulators and criminal authorities in India, Singapore, Canada, and Sweden have worked with us on investigations and enforcement.

Some of the private partnerships have been just as remarkable. I mentioned the USTelecom Robocall Traceback Initiative, which has been invaluable in leading us to the source of illegal robocalls. Our partnerships with the BBB and AARP have enabled us to reach literally millions of consumers with our educational message. In fact, one AARP presentation early in the pandemic was viewed by more than 850,000 people.

We are always open to new ideas about how to better educate and protect consumers from these pernicious COVID-related scams. And I look forward to today's conversation on this topic.

Thank you for the opportunity to testify. I welcome your questions.

[The prepared statement of Mr. Smith follows:]

PREPARED STATEMENT OF ANDREW SMITH, DIRECTOR, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION

## I. INTRODUCTION

Chairman Moran, Ranking Member Blumenthal, and members of the Subcommittee, I am Andrew Smith, Director of the Federal Trade Commission's ("FTC" or "Commission") Bureau of Consumer Protection. I am pleased to appear before you today to discuss consumer protection issues arising from the COVID-19 pandemic.<sup>1</sup>

The FTC is a highly productive, bipartisan independent agency with a broad mission. It is the only Federal agency with jurisdiction to both protect consumers and maintain competition in most sectors of the economy.<sup>2</sup> In fulfilling its consumer protection mission, the agency enforces laws that prohibit business practices that are unfair or deceptive to consumers, being mindful not to impede legitimate business activity. The FTC also educates consumers and businesses to encourage informed consumer choices and compliance with the law. Through its research, reports, and policy work, the FTC further promotes an honest and competitive marketplace.

On March 13, 2020, the President declared a national emergency in response to the global outbreak of the "Coronavirus Disease 2019" ("COVID-19" or

<sup>1</sup>This written statement presents the views of the Federal Trade Commission. My oral statement and responses to questions are my own and do not necessarily reflect the views of the Commission or any Commissioner.

<sup>2</sup>The FTC has broad law enforcement responsibilities under the Federal Trade Commission Act, 15 U.S.C. § 41 *et seq.*, and enforces a wide variety of other laws ranging from the Clayton Act to the Fair Credit Reporting Act. In total, the Commission has enforcement or administrative responsibilities under more than 70 laws. See <https://www.ftc.gov/enforcement/statutes>.

“coronavirus”).<sup>3</sup> The FTC has worked aggressively to combat consumer protection issues arising from the COVID-19 pandemic. In late March, Chairman Joseph Simons stated that the FTC would “not tolerate businesses seeking to take advantage of consumers’ concerns and fears regarding [the] coronavirus disease, exigent circumstances, or financial distress.”<sup>4</sup> And we have not.

To date, the FTC has received over 131,419 consumer complaints relating to COVID-19, including complaints about the government’s economic impact payments, or so-called stimulus checks.<sup>5</sup> In addition, the FTC is monitoring the marketplace for unsubstantiated health claims, robocalls, privacy and data security concerns, sham charities, online shopping fraud, phishing scams, work at home scams, credit scams, and fake mortgage and student loan relief schemes. This also includes monitoring of a variety of other scams related to the economic fallout from the COVID-19 pandemic, including government imposters attempting to scam consumers out of their stimulus checks.

While the FTC has quickly pivoted to address aggressively the myriad of COVID-related scams, the agency has continued its extensive consumer protection work. Since early March, the FTC has distributed \$40 million in redress<sup>6</sup> in more than 10 cases. In addition, our partners at the Department of Justice distributed another \$153 million from our multi-agency settlement with Western Union.<sup>7</sup> We have published rulemaking notices,<sup>8</sup> workshop reports,<sup>9</sup> reports to Congress,<sup>10</sup> data spot-

<sup>3</sup>President Donald J. Trump, *Proclamation on Declaring a National Emergency Concerning the Novel Coronavirus Disease (COVID-19)* (Mar. 13, 2020), available at <https://www.whitehouse.gov/presidential-actions/proclamation-declaring-national-emergency-concerning-novel-coronavirus-disease-covid-19-outbreak/>.

<sup>4</sup>FTC Press Release, *FTC Chairman Joe Simons Outlines the Agency’s Approach to Safeguarding Consumers During the Coronavirus Pandemic* (Mar. 26, 2020), <https://www.ftc.gov/news-events/press-releases/2020/03/ftc-chairman-joe-simons-outlines-agencys-approach-safe-guarding>.

<sup>5</sup>See FTC, *FTC COVID-19 and Stimulus Reports: Consumer Sentinel Network Reports*, <https://public.tableau.com/profile/federal.trade.commission#!/vizhome/COVID-19andStimulusReports/Map> (last visited July 6, 2020).

<sup>6</sup>In fact, between July 1, 2018 and December 31, 2019, FTC actions resulted in \$1.2 billion in refunds to consumers, including \$542.9 million in refunds the FTC sent to consumers and the remainder sent through self-administered redress programs. Of the \$556.9 million the FTC disbursed during that time, more than 97 percent ended up in consumers’ pockets, with 1.6 percent spent on administrative costs and less than 1 percent sent to the U.S. Treasury (either because a refund program was not feasible or because there was money left over after the refund program was complete). See FTC, *Data on Refunds to Consumers*, <https://www.ftc.gov/enforcement/cases-proceedings/refunds/data-refunds-consumers> (last visited July 6, 2020).

<sup>7</sup>See FTC Press Release, *First Round of Refunds Totaling \$153 Million Sent to Consumers As a Result of Multi-Agency Case Against Western Union* (Mar. 10, 2020), <https://www.ftc.gov/news-events/press-releases/2020/03/first-round-refunds-totaling-153-million-sent-consumers-result>.

<sup>8</sup>See FTC Press Release, *FTC Announces Final Amendments to the Agency’s Contact Lens Rule* (June 23, 2020), <https://www.ftc.gov/news-events/press-releases/2020/06/ftc-announces-final-amendments-agencys-contact-lens-rule>; FTC Press Release, *FTC Seeks Public Comment on Proposed Repeal of the Care Labeling Rule* (June 22, 2020), <https://www.ftc.gov/news-events/press-releases/2020/06/ftc-seeks-public-comment-proposed-repeal-care-labeling-rule>; FTC Press Release, *FTC Issues Staff Report on Made in the USA Workshop, Seeks Comment on Related Proposed Rulemaking for Labeling Rule* (June 22, 2020), <https://www.ftc.gov/news-events/press-releases/2020/06/ftc-issues-staff-report-on-made-in-usa-workshop>; FTC Press Release, *FTC Seeks Comment as Part of Review of Health Breach Notification Rule* (May 8, 2020), <https://www.ftc.gov/news-events/press-releases/2020/05/ftc-seeks-comment-part-review-health-breach-notification-rule>; FTC Press Release, *FTC Seeks Comments on Proposed Changes to the Energy Labeling Rule* (Mar. 27, 2020), <https://www.ftc.gov/news-events/press-releases/2020/03/ftc-seeks-comments-proposed-changes-energy-labeling-rule>.

<sup>9</sup>See FTC Press Release, *FTC Issues Staff Report on Made in the USA Workshop, Seeks Comment on Related Proposed Rulemaking for Labeling Rule* (June 22, 2020), <https://www.ftc.gov/news-events/press-releases/2020/06/ftc-issues-staff-report-on-made-in-usa-workshop>; FTC Press Release, *FTC Staff Perspective Recaps Online Events Tickets Workshop* (May 7, 2020), <https://www.ftc.gov/news-events/press-releases/2020/05/ftc-staff-perspective-recaps-online-event-tickets-workshop>.

<sup>10</sup>See FTC Press Release, *FTC Updates Congress on Efforts to Educate Consumers about Their FCRA Rights* (May 5, 2020), <https://www.ftc.gov/news-events/press-releases/2020/05/ftc-updates-congress-efforts-educate-consumers-about-their-fcra>; FTC Press Release, *FTC Sends Report to Congress on Retailers’ Shipping Policies* (Apr. 17, 2020), <https://www.ftc.gov/news-events/press-releases/2020/04/ftc-sends-report-congress-retailers-shipping-policies>. See also FTC Press Release, *FTC Staff Provides Annual Letter to CFPB On Fair Debt Collection Practices Act Activities* (Mar. 20, 2020), <https://www.ftc.gov/news-events/press-releases/2020/03/ftc-staff-provides-annual-letter-cfpb-fair-debt-collection> (providing information to CFPB for Congressional Report).

lights,<sup>11</sup> and the new [econsumer.gov](https://www.consumer.gov) interactive dashboards.<sup>12</sup> The FTC also has announced complaints or settlements in more than 30 law enforcement matters, including settlements that will return more than \$225 million to consumers,<sup>13</sup> privacy cases,<sup>14</sup> national advertising cases,<sup>15</sup> fraud cases,<sup>16</sup> payment processor cases,<sup>17</sup> fi-

<sup>11</sup> See FTC Press Release, *Active Duty Servicemembers are More Likely to Report Identity Theft than Other Adults, New FTC Data Shows* (May 21, 2020), <https://www.ftc.gov/news-events/press-releases/2020/05/active-duty-servicemembers-are-more-likely-report-identity-theft>.

<sup>12</sup> See generally <https://econsumer.gov>.

<sup>13</sup> See FTC Press Release, *Worldwide Payment Processor and Payments Industry Executive to Pay \$40.2 Million to Settle FTC Charges of Assisting Fraudulent Schemes and Credit Card Laundering* (May 19, 2020), <https://www.ftc.gov/news-events/press-releases/2020/05/worldwide-payment-processor-payments-industry-executive-pay-402>; FTC Press Release, *FTC Halts Online Subscription Scheme that Deceived People with “Free Trial Offers”* (May 8, 2020), <https://www.ftc.gov/news-events/press-releases/2020/05/ftc-halts-online-subscription-scheme-deceived-people-free-trial>; FTC Press Release, *Fashion Nova Will Pay \$9.3 Million for Consumer Refunds To Settle FTC Charges It Violated Rules On Shipping, Refunds* (Apr. 21, 2020), <https://www.ftc.gov/news-events/press-releases/2020/04/fashion-nova-will-pay-93-million-consumer-refunds-settle-ftc>; FTC Press Release, *Rent-To-Own Payment Plan Company Progressive Leasing Will Pay \$175 Million to Settle FTC Charges It Deceived Consumers About Pricing* (Apr. 20, 2020), <https://www.ftc.gov/news-events/press-releases/2020/04/rent-own-payment-plan-company-progressive-leasing-will-pay-175>; FTC Press Release, *Student Loan Debt Relief Companies Agree to Settle FTC Charges They Falsely Promised to Lower or Eliminate Consumers’ Student Loans* (Mar. 30, 2020), <https://www.ftc.gov/news-events/press-releases/2020/03/student-loan-debt-relief-companies-agree-settle-ftc-charges-they>.

<sup>14</sup> See FTC Press Release, *Swiss Digital Game Developer Settles FTC Allegations that it Falsely Claimed it was a Member of COPPA Safe Harbor Program* (May 19, 2020), <https://www.ftc.gov/news-events/press-releases/2020/05/swiss-digital-game-developer-settles-ftc-allegations-it-falsely>; FTC Press Release, *Medical Diagnostic Device Maker Settles Allegations that it Misled Consumers about its Participation in the EU-U.S. Privacy Shield* (Mar. 30, 2020), <https://www.ftc.gov/news-events/press-releases/2020/03/medical-diagnostic-device-maker-settles-allegations-it-misled>.

<sup>15</sup> See FTC Press Release, *Williams-Sonoma, Inc. Settles with FTC, Agrees to Stop Making Overly Broad and Misleading “Made in USA” Claims about Houseware and Furniture Products* (Mar. 30, 2020), <https://www.ftc.gov/news-events/press-releases/2020/03/williams-sonoma-inc-settles-ftc-agrees-stop-making-overly-broad>; FTC Press Release, *FTC Acts to Stop False and Unsubstantiated Claims for Wagner OEX Brake Pads* (Mar. 25, 2020), <https://www.ftc.gov/news-events/press-releases/2020/03/ftc-acts-stop-false-unsubstantiated-claims-wagner-oex-brake-pads>.

<sup>16</sup> See FTC Press Release, *Operators of Business Coaching Scheme Will Pay At Least \$1.2 Million to Settle FTC Charges They Deceived Consumers Starting New Internet-based Businesses* (May 13, 2020), <https://www.ftc.gov/news-events/press-releases/2020/05/operators-business-coaching-scheme-will-pay-least-12-million>; FTC Press Release, *FTC Files Complaint Alleging Telemarketers and Debt Collectors Worked Together to Bilk Organizations for Subscriptions and Books They Never Ordered* (May 13, 2020), <https://www.ftc.gov/news-events/press-releases/2020/05/ftc-files-complaint-alleging-telemarketers-debt-collectors-worked>; FTC Press Release, *FTC Halts Online Subscription Scheme that Deceived People with “Free Trial” Offers* (May 8, 2020), <https://www.ftc.gov/news-events/press-releases/2020/05/ftc-halts-online-subscription-scheme-deceived-people-free-trial>; FTC Press Release, *FTC Obtains Preliminary Injunction Against Investor Training Scheme Online Trading Academy* (Apr. 7, 2020), <https://www.ftc.gov/news-events/press-releases/2020/04/ftc-obtains-preliminary-injunction-against-investor-training>; FTC Press Release, *Affiliate Marketers to Pay More Than \$4 Million to Settle Charges that They Promoted a Fraudulent Business Coaching and Investment Scheme* (Mar. 5, 2020), <https://www.ftc.gov/news-events/press-releases/2020/03/affiliate-marketers-pay-more-4-million-settle-charges-they>.

<sup>17</sup> See FTC Press Release, *Rogue Payment Processor that Helped Perpetuate Multiple Scams Is Banned from the Payment Processing Business Under FTC Settlement* (June 9, 2020), <https://www.ftc.gov/news-events/press-releases/2020/06/rogue-payment-processor-helped-perpetuate-multiple-scams-banned>; FTC Press Release, *Payment Processor for MOBE Business Coaching Scheme Settles FTC Charges* (June 1, 2020), <https://www.ftc.gov/news-events/press-releases/2020/06/payment-processor-mobe-business-coaching-scheme-settles-ftc>; FTC Press Release, *Worldwide Payment Processor and Payments Industry Executive to Pay \$40.2 Million to Settle FTC Charges of Assisting Fraudulent Schemes and Credit Card Laundering* (May 19, 2020), <https://www.ftc.gov/news-events/press-releases/2020/05/worldwide-payment-processor-payments-industry-executive-pay-402>; FTC Press Release, *Credit Card Launderer for Tech Support Scams to Pay \$6.75 Million to Settle FTC Charges* (Apr. 22, 2020), <https://www.ftc.gov/news-events/press-releases/2020/04/credit-card-launderer-tech-support-scams-pay-675-million-settle>.

financial services cases,<sup>18</sup> rule violations,<sup>19</sup> civil penalty cases,<sup>20</sup> a data security case,<sup>21</sup> health advertising cases,<sup>22</sup> and our first fair lending case in 10 years.<sup>23</sup> This is all to say that the Commission's extensive COVID-related work has not taken the Commission's attention away from its continued dedication to American consumers and the non-COVID-related hardships they are facing.

As always, the FTC appreciates your support of our consumer protection mission. An essential part of that mission is getting back to consumers money wrongly taken from them. Unfortunately, our ability to do so has been threatened or curtailed by recent judicial decisions, making it harder for the FTC to get consumer redress, including in coronavirus-related scam cases. We therefore respectfully request that Congress clarify the agency's statutory authority to obtain complete consumer redress under Section 13(b) of the FTC Act. Section 13(b) says the FTC can seek "per-

<sup>18</sup> See FTC Press Release, *FTC Halts Deceptive Payday Lender That Took Millions From Consumers' Accounts Without Authorization* (May 22, 2020), <https://www.ftc.gov/news-events/press-releases/2020/05/ftc-halts-deceptive-payday-lender-took-millions-consumers>; FTC Press Release, *Student Loan Debt Relief Companies Agree to Settle FTC Charges They Falsely Promised to Lower or Eliminate Consumers' Student Loans* (Mar. 30, 2020), <https://www.ftc.gov/news-events/press-releases/2020/03/student-loan-debt-relief-companies-agree-settle-ftc-charges-they>; FTC Press Release, *Health Center, Inc. Settles FTC Allegations That It Targeted Older Consumers With Deceptive Claims for Health and Wellness Products* (Mar. 19, 2020), <https://www.ftc.gov/news-events/press-releases/2020/03/health-center-inc-settles-ftc-allegations-it-targeted-older>; FTC Press Release, *Credit Repair Company Settles FTC Charges It Deceived Consumers By Telling Them "Piggybacking" on Others' Credit Could Boost Scores* (Mar. 9, 2020), <https://www.ftc.gov/news-events/press-releases/2020/03/credit-repair-company-settles-ftc-charges-it-deceived-consumers>.

<sup>19</sup> See FTC Press Release, *Developer of Apps Popular with Children Agrees to Settle FTC Allegations It Illegally Collected Kids' Data without Parental Consent* (June 4, 2020), <https://www.ftc.gov/news-events/press-releases/2020/06/developer-apps-popular-children-agrees-settle-ftc-allegations-it>; FTC Press Release, *Auto Dealership Bronx Honda, General Manager to Pay \$1.5 Million to Settle FTC Charges They Discriminated Against African-American, Hispanic Car Buyers* (May 27, 2020), <https://www.ftc.gov/news-events/press-releases/2020/05/bronx-honda-to-pay-over-1-million-to-settle-charges>; FTC Press Release, *Credit Card Launderer for Tech Support Scams to Pay \$6.75 Million to Settle FTC Charges* (Apr. 22, 2020), <https://www.ftc.gov/news-events/press-releases/2020/04/credit-card-launderer-tech-support-scams-pay-675-million-settle>; FTC Press Release, *Fashion Nova Will Pay \$9.3 Million for Consumer Refunds To Settle FTC Charges It Violated Rules on Shipping, Refunds* (Apr. 21, 2020), <https://www.ftc.gov/news-events/press-releases/2020/04/fashion-nova-will-pay-93-million-consumer-refunds-settle-ftc>; FTC Press Release, *Student Loan Debt Relief Companies Agree to Settle FTC Charges They Falsely Promised to Lower or Eliminate Consumers' Student Loans* (Mar. 30, 2020), <https://www.ftc.gov/news-events/press-releases/2020/03/student-loan-debt-relief-companies-agree-settle-ftc-charges-they>; FTC Press Release, *Credit Repair Company Settles FTC Charges It Deceived Consumers By Telling Them "Piggybacking" on Others' Credit Could Boost Scores* (Mar. 9, 2020), <https://www.ftc.gov/news-events/press-releases/2020/03/credit-repair-company-settles-ftc-charges-it-deceived-consumers>.

<sup>20</sup> See FTC Press Release, *Developer of Apps Popular with Children Agrees to Settle FTC Allegations It Illegally Collected Kids' Data without Parental Consent* (June 4, 2020), <https://www.ftc.gov/news-events/press-releases/2020/06/developer-apps-popular-children-agrees-settle-ftc-allegations-it>; FTC Press Release, *FTC Reaches Settlement with Kohl's over Allegations it Failed to Provide Victims with Information Related to Identity Theft* (June 10, 2020), <https://www.ftc.gov/news-events/press-releases/2020/06/ftc-reaches-settlement-kohls-over-allegations-it-failed-provide>.

<sup>21</sup> See FTC Press Release, *Canadian Maker of Smart Locks Settles FTC Allegations that It Deceived Consumers about Its Security Practices* (Apr. 6, 2020), <https://www.ftc.gov/news-events/press-releases/2020/04/canadian-maker-smart-locks-settles-ftc-allegations-it-deceived>.

<sup>22</sup> See FTC Press Release, *FTC Puts an End to Deceptive Advertising of Light Therapy Device* (June 25, 2020), <https://www.ftc.gov/news-events/press-releases/2020/06/ftc-puts-end-deceptive-advertising-light-therapy-device>; FTC Press Release, *FTC Takes Action to Stop Direct Mail Pill Marketers' Unproven Health Claims* (Apr. 20, 2020), <https://www.ftc.gov/news-events/press-releases/2020/04/ftc-takes-action-stop-direct-mail-pill-marketers-unproven-health>; FTC Press Release, *FTC Halts Bogus Claims about "Miracle" Supplement for Older Adults* (Apr. 16, 2020), <https://www.ftc.gov/news-events/press-releases/2020/04/ftc-halts-bogus-claims-about-miracle-supplement-older-adults>; FTC Press Release, *Health Center, Inc. Settles FTC Allegations That It Targeted Older Consumers With Deceptive Claims for Health and Wellness Products* (Mar. 19, 2020), <https://www.ftc.gov/news-events/press-releases/2020/03/health-center-inc-settles-ftc-allegations-it-targeted-older>; FTC Press Release, *Tea Marketer Misled Consumers, Didn't Adequately Disclose Payments to Well-Known Influencers, FTC Alleges* (Mar. 6, 2020), <https://www.ftc.gov/news-events/press-releases/2020/03/tea-marketer-misled-consumers-didnt-adequately-disclose-payments>; FTC Press Release, *Marketers of Pain Relief Device Settle FTC False Advertising Complaint* (Mar. 4, 2020), <https://www.ftc.gov/news-events/press-releases/2020/03/marketers-pain-relief-device-settle-ftc-false-advertising>.

<sup>23</sup> See FTC Press Release, *Auto Dealership Bronx Honda, General Manager to Pay \$1.5 Million to Settle FTC Charges They Discriminated Against African-American, Hispanic Car Buyers* (May 27, 2020), <https://www.ftc.gov/news-events/press-releases/2020/05/bronx-honda-to-pay-over-1-million-to-settle-charges>.

manent injunctions,” and for decades, courts interpreted that language to mean that the FTC could secure equitable monetary remedies, including restitution to consumers and disgorgement of ill-gotten gains. One recent decision from the Seventh Circuit held that Section 13(b) was limited to injunctions and so did not allow monetary remedies at all.<sup>24</sup> The Supreme Court has agreed to hear that case and another case, from the Ninth Circuit, that ruled we are entitled to monetary equitable relief.

<sup>25</sup> We expect the Court to resolve this issue by next summer. A decision last year from the Third Circuit held that the FTC could bring cases under Section 13(b) only if the illegal acts were ongoing or impending, limiting our ability to pursue past illegality.<sup>26</sup> And the Supreme Court’s recent *Liu* decision may place limitations on the amount of money we can obtain from wrongdoers and ultimately return to consumers.<sup>27</sup> In short, our ability to get full redress for consumers is in peril. Congress should act now to preserve the FTC’s ability to restore to consumers money they lose to scammers and fraudsters.

In addition, the Commission’s primary source of legal authority in the privacy and data security space is Section 5 of the FTC Act, which prohibits deceptive or unfair commercial practices.<sup>28</sup> Section 5, however, is not without its limitations. For example, Section 5 does not allow the Commission to seek civil penalties for the first offense. It also excludes non-profits and common carriers from the Commission’s authority, even when the acts or practices of these market participants have serious implications for consumer privacy and data security. To better equip the Commission to meet its statutory mission to protect consumers, we urge Congress to enact privacy and data security legislation, enforceable by the FTC, which grants the agency civil penalty authority, targeted Administrative Procedure Act rulemaking authority, and jurisdiction over non-profits and common carriers.<sup>29</sup>

## II. COVID-19 HEALTH FRAUDS

It is often the case that, following reports of a health scare, deceptive advertising or marketing touting “miracle cures” quickly emerge. The COVID-19 pandemic has put this cause and effect scenario into overdrive. Although some of these supposed “treatments” seem facially preposterous, it is not uncommon for consumers in distress to be willing to try (and spend) anything in the hopes that it will protect them or their families from sickness or death.

Given the breadth of false treatment claims we have seen regarding COVID-19, the FTC determined that the fastest way to get these false treatment claims taken down is to pursue a rigorous warning letter program. To date, the FTC and the Food and Drug Administration (“FDA”) have issued 65 joint warning letters to marketers regarding claims that their products will treat, cure, or prevent COVID-19, and there are additional joint warning letters in the pipeline.<sup>30</sup> The FTC also has issued its own 190 warning letters to additional marketers.<sup>31</sup> The letters warn recipients that their conduct is likely to be unlawful, that they could face serious legal consequences if they do not immediately stop, and require a response to the FTC within 48 hours. Overwhelmingly, companies that have received FTC warning letters these past few months have taken quick steps to correct their problematic claims. As a result, warning letters are frequently the most rapid and efficient means to address the problem. However, when a warning letter does not work, or is not appropriate given the conduct at issue, the FTC has pursued law enforcement.

<sup>24</sup> See *Fed. Trade Comm’n v. Credit Bureau Ctr., LLC*, 937 F.3d 764 (7th Cir. 2019).

<sup>25</sup> *Fed. Trade Comm’n v. Credit Bureau Ctr., LLC*, 937 F.3d 764 (7th Cir. 2019), cert. granted, No. 19–825 (July 9, 2020); *AMG Cap. Mgmt., LLC v. Fed. Trade Comm’n*, 910 F.3d 417 (9th Cir. 2018), cert. granted, No. 19–508 (July 9, 2020).

<sup>26</sup> See *Fed. Trade Comm’n v. Shire ViroPharma, Inc.*, 917 F.3d 147 (3rd Cir. 2019).

<sup>27</sup> See *Liu v. Sec. Exch. Comm’n*, 140 S.Ct. 1936 (2020).

<sup>28</sup> 15 U.S.C. § 45. The Commission also enforces sector-specific statutes containing privacy and data security provisions, such as the Gramm-Leach-Bliley Act (“GLB Act”), Pub. L. No. 106–102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 and 15 U.S.C.), and the Children’s Online Privacy Protection Act (“COPPA”), 15 U.S.C. §§ 6501–6506.

<sup>29</sup> Commissioner Phillips supports congressional efforts to consider consumer data privacy legislation. He believes legislation should be based on harms that Congress agrees warrant a remedy, and that tools like penalties and rulemaking should be calibrated carefully to address those harms. Commissioner Phillips believes Congress should also give appropriate consideration to the trade-offs involved in new regulation, and, with regard to rulemaking, reserve to itself fundamental value judgments appropriately made by the legislature. Finally, Commissioner Phillips believes data security legislation is a critical step Congress should also take to protect consumer privacy.

<sup>30</sup> See generally <https://www.ftc.gov/coronavirus/enforcement/warning-letters>.

<sup>31</sup> *Id.* The FTC issues its own warning letters to entities selling products that are outside the FDA’s jurisdiction.

The FTC's action against Marc Ching, doing business as Whole Leaf Organics, is one example.<sup>32</sup> Mr. Ching had previously received a letter from the FDA warning him that he was making unapproved drug claims by claiming that his cannabidiol ("CBD") products were intended for use in the treatment or prevention of diseases. Not only did Mr. Ching fail to remove the unapproved CBD claims from his website, he *added* COVID-19 claims for a Vitamin C and herbal extracts product during the pandemic.<sup>33</sup> We knew that with these facts, a warning letter was not appropriate. On April 22, the FTC issued an administrative complaint alleging that Mr. Ching deceptively advertised a supplement as a clinically-proven immunity booster that prevents and treats COVID-19.<sup>34</sup> Two days later, the FTC filed a Federal complaint seeking preliminary relief containing the same allegations about Mr. Ching's health claims. By April 26, Mr. Ching had agreed to the Federal preliminary order, barring him from claiming that his products were effective at treating, preventing, or reducing the risk of COVID-19 for the duration of the administrative proceeding. Mr. Ching subsequently agreed to settle the administrative case with an order barring his false and unsubstantiated health claims, and requiring him to send written notices to customers and retailers that his products would not treat, prevent, or reduce the risk of COVID-19, or prevent or treat cancer, and inform them of his settlement with the Commission.<sup>35</sup>

### III. MULTI-LEVEL MARKETING COMPANIES

The FTC also has issued warning letters to major multi-level marketing companies ("MLMs") regarding COVID-19 prevention or treatment claims made by the MLM and/or its business opportunity participants.<sup>36</sup> In addition to warning the MLMs regarding the prevention or treatment claims, we also warned them that they are responsible for their earnings claims as well as earnings claims made by their business opportunity participants and representatives.<sup>37</sup>

To date, the FTC has sent 12 warning letters to MLMs regarding prevention or treatment claims, earning claims, or both, made by the MLMs themselves,<sup>38</sup> or by business opportunity representatives or participants on their behalf.<sup>39</sup> Telling a con-

<sup>32</sup> *U.S. v. Marc Ching*, No. 2:20-cv-03775 (C.D. Cal. 2020), <https://www.ftc.gov/enforcement/cases-proceedings/202-3110/whole-leaf-organics>; *Marc Ching*, No. D9394 (administrative complaint filed Apr. 27, 2020), <https://www.ftc.gov/enforcement/cases-proceedings/202-3110/marc-ching-matter>.

<sup>33</sup> Mr. Ching sold a supplement, called "Thrive," and advertised that it was "the perfect way to strengthen your immunity against pathogens like, 'COVID-19,' THE CORONAVIRUS." (Emphasis in original). *Marc Ching*, No. D9394 (administrative complaint, Exhibit A), [https://www.ftc.gov/system/files/documents/cases/d09394\\_administrative\\_part\\_iii\\_complaint.pdf](https://www.ftc.gov/system/files/documents/cases/d09394_administrative_part_iii_complaint.pdf).

<sup>34</sup> The complaint also alleged that Mr. Ching deceptively advertised that his CBD products would prevent and treat cancer, and that clinical studies established the efficacy of these products. *Id.*

<sup>35</sup> FTC Press Release, *FTC Order Stops the Marketer of "Thrive" Supplement from Making Baseless Claims It Can Treat, Prevent, or Reduce the Risks from COVID-19* (July 10, 2020), <https://www.ftc.gov/news-events/press-releases/2020/07/ftc-order-stops-marketer-thrive-supplement-making-baseless-claims>.

<sup>36</sup> See FTC Press Release, *FTC Sends Second Round of Warning Letters to Multi-Level Marketers Regarding Coronavirus Related Health and Earnings Claims* (June 5, 2020), <https://www.ftc.gov/news-events/press-releases/2020/06/second-round-warning-letters-to-mlms-regarding-coronavirus> (letters to Isagenix International LLC, The Juice Plus+ Company, Youngevity International, Inc., Vivri USA, LLC, and Plexus Worldwide, LLC included health claims); FTC Press Release, *FTC Sends Warning Letters to Multi-Level Marketers Regarding Health and Earnings Claims They or Their Participants are Making Related to Coronavirus* (Apr. 24, 2020), <https://www.ftc.gov/news-events/press-releases/2020/04/ftc-sends-warning-letters-multi-level-marketers-regarding-health> (letters to doTERRA International, Inc., Pruvit Ventures, Inc., Total Life Changes, LLC, Tranont, Modere, Inc., Arbonne International, LLC, and Zurvita, Inc. included health claims).

<sup>37</sup> See also FTC, *Business Guidance Concerning Multi-Level Marketing* (Jan. 2018), <https://www.ftc.gov/tips-advice/business-center/guidance/business-guidance-concerning-multi-level-marketing>.

<sup>38</sup> FTC Press Release, *FTC Sends Warning Letters to Multi-Level Marketers Regarding Health and Earnings Claims They or Their Participants are Making Related to Coronavirus* (Apr. 24, 2020), <https://www.ftc.gov/news-events/press-releases/2020/04/ftc-sends-warning-letters-multi-level-marketers-regarding-health> (letter to It Works Marketing, Inc.).

<sup>39</sup> See FTC Press Release, *FTC Sends Second Round of Warning Letters to Multi-Level Marketers Regarding Coronavirus Related Health and Earnings Claims* (June 5, 2020), <https://www.ftc.gov/news-events/press-releases/2020/06/second-round-warning-letters-to-mlms-regarding-coronavirus> (letters to Isagenix International LLC, The Juice Plus+ Company, and Melaleuca, Inc. included earnings claims); FTC Press Release, *FTC Sends Warning Letters to Multi-Level Marketers Regarding Health and Earnings Claims They or Their Participants are Making Related to Coronavirus* (Apr. 24, 2020), <https://www.ftc.gov/news-events/press-releases/2020/04/ftc-sends-warning-letters-multi-level-marketers-regarding-health> (letters to doTERRA

sumer that by joining an MLM business venture they can earn a certain amount of money in a month, or obtain “financial freedom,” when it is unlikely they can do so, is unlawful. The need to address such claims is pressing because consumers are facing extreme economic and employment uncertainty due to the COVID-19 pandemic. The FTC’s warning letters make it clear that misrepresenting a consumer’s potential earnings will not be tolerated.

#### IV. COVID-19 FINANCIAL VULNERABILITY FRAUDS

Alongside the health concerns presented by COVID-19, many consumers are facing substantial economic and financial hardships because of the pandemic. These are also dire times for small businesses. The FTC has been on the lookout for frauds targeting financially vulnerable consumers and small businesses, and is pursuing warning letters and law enforcement to protect them from further financial harm.

Millions of American consumers lost their jobs because of the pandemic. With families to support, many consumers are seeking alternative ways to make money. In addition to the MLM effort outlined above, we have redoubled our efforts to identify scam business opportunities that look better than they are.

The FTC also recognizes that the financial hardships caused by the pandemic are not just limited to consumers. Small businesses have sought out relief and loans through the Paycheck Protection Program (PPP) or other programs authorized by the Coronavirus Aid, Relief, and Economic Security (CARES) Act.<sup>40</sup> To date, the FTC and the Small Business Administration (“SBA”) have issued 8 warning letters to companies making claims that could lead consumers and small businesses to believe these companies are somehow affiliated with the SBA, that consumers and small businesses could get PPP loans by applying on their website, or otherwise misleading small business about Federal loans or other temporary small business relief.<sup>41</sup> As with deceptive health claims, the FTC believes that the fastest way to take down these false claims is by issuing warning letters. However, as always, in some cases, the FTC will pursue law enforcement. For example, on April 17, 2020, the FTC filed a complaint against one such company that was posing as an approved PPP lender.<sup>42</sup> The FTC will continue to monitor the marketplace and will take action where appropriate to combat such frauds.

#### V. ONLINE SHOPPING FRAUD

“Online shopping” has recently become the leading source of coronavirus-related consumer complaints in our Consumer Sentinel database.<sup>43</sup> These complaints are, in part, about merchants that offer for sale masks, personal protective equipment, and related products, but then do not ship the products, fail to meet their delivery promises, or ship products other than those advertised, and fail to provide refunds to consumers. We recently brought an expedited enforcement action—in conjunction with criminal authorities who executed a search warrant at the same time<sup>44</sup>—and are seeking additional actions where it would be appropriate to combat such frauds in conjunction with criminal authorities. Working together with criminal authorities, we can get effective injunctive relief and compliance monitoring quickly.

#### VI. COVID-19 SPOOFING/IMPOSTER SCAMS

Aside from scams targeting health and financial vulnerabilities caused by the pandemic, the FTC has responded to other coronavirus-related fraudulent behavior.

The FTC has issued warning letters to 15 Voice over Internet Protocol (VoIP) service providers and other companies, warning them that “assisting and facilitating” illegal telemarketing or robocalls related to the COVID-19 pandemic is

International, Inc., Pruvit Ventures, Inc., Total Life Changes, LLC, Tranont, Modere, Inc., Arbonne International, LLC, IDLife, LLC, and Rodan & Fields, LLC included earnings claims).

<sup>40</sup> P.L. 116–136.

<sup>41</sup> See FTC Press Release, *FTC and SBA Warn Six Companies to Stop Potentially Misleading Marketing Aimed at Small Businesses Seeking Coronavirus Relief Loans* (June 24, 2020), <https://edit.ftc.gov/news-events/press-releases/2020/06/ftc-sba-warn-six-companies-stop-potentially-misleading-marketing>; FTC Press Release, *FTC and SBA Warn Operator of SBA.com and Lead Generator Lendio to Stop Potentially Misleading Coronavirus Relief Loan Marketing* (May 18, 2020), <https://www.ftc.gov/news-events/press-releases/2020/05/ftc-sba-warn-operator-sbacom-lead-generator-lendio-stop>.

<sup>42</sup> *FTC v. Ponte Investments, LLC*, No. 1:20-cv-00177 (D.R.I. Apr. 17, 2020), <https://www.ftc.gov/enforcement/cases-proceedings/202-3115/ponte-investments-llc>.

<sup>43</sup> See FTC Consumer Sentinel Network Reports, *FTC COVID-19 and Stimulus Reports*, <https://public.tableau.com/profile/federal.trade.commission#!/vizhome/COVID-19andStimulusReports/Map> (last visited July 6, 2020).

<sup>44</sup> FTC Press Release, *FTC Takes Action against Marketer That Falsely Promised Consumers Next Day Shipping of Facemasks and Other Personal Protective Equipment* (July 8, 2020), <https://www.ftc.gov/news-events/press-releases/2020/07/ftc-takes-action-against-marketer-that-falsely-promised-next-day-shipping>.

against the law.<sup>45</sup> The Federal Communications Commission joined the FTC on 6 of these warning letters.<sup>46</sup> Many of these calls prey upon consumers' fear of the virus to perpetrate scams or sow disinformation. The letters stress that combatting illegal telemarketing and robocalls is a top priority of the Commission.<sup>47</sup>

The agency will continue to review complaints and monitor the marketplace to keep abreast of evolving scams and make sure that consumers have the most up-to-date information and advice possible.

## VII. COVID-19 CONSUMER EDUCATION AND OUTREACH

The FTC has worked aggressively to educate consumers of all ages about coronavirus-related scams from the onset of this crisis. FTC staff across the Bureau of Consumer Protection (including the eight regional offices) conduct national and local outreach with partners to reach a variety of audiences, including older consumers, ethnic media, housing organizations, and re-entry groups by using webinars, tele-town halls, Twitter chats, Facebook Live events, as well as interviews with local and national media. During the pandemic, FTC staff have participated in hundreds of virtual webinars, presentations, and interviews—in English, Spanish, and Mandarin.<sup>48</sup>

On February 10, the FTC issued its first consumer alert warning about the potential scams that come with widespread health concerns like the COVID-19 pandemic.<sup>49</sup> The FTC also developed a multi-media campaign, complete with a dedicated website in response to the COVID-19 pandemic.<sup>50</sup> This page contains a library of more than 96 consumer and business posts and scam alerts on topics ranging from stimulus payments and health claims to charity fraud, government imposter scams, and misinformation and rumors.<sup>51</sup> The FTC's coronavirus webpage also includes a free one-page infographic that other organizations can share with consumers.<sup>52</sup> FTC staff regularly updates the page, linking to related consumer and business alerts, law enforcement actions, consumer report data, and other details about the FTC's efforts to combat coronavirus-related scams and educate consumers. More than 365,000 businesses and consumers receive FTC alerts.<sup>53</sup> All resources on the FTC's website are free for consumers and organizations—including any member

<sup>45</sup> FTC Press Release, *FTC and FCC Sent Joint Letters to Additional VoIP Providers Warning against 'Routing and Transmitting' Illegal Coronavirus-related Robocalls* (May 20, 2020), <https://www.ftc.gov/news-events/press-releases/2020/05/ftc-fcc-send-joint-letters-additional-voip-providers-warning>; FTC Press Release, *FTC and FCC Send Joint Letters to VoIP Service Providers Warning against 'Routing and Transmitting' Illegal Coronavirus-related Robocalls* (Apr. 3, 2020), <https://www.ftc.gov/news-events/press-releases/2020/04/ftc-fcc-send-joint-letters-voip-service-providers-warning-against>; FTC Press Release, *FTC Warns Nine VoIP Service Providers and Other Companies against 'Assisting and Facilitating' Illegal Coronavirus-related Telemarketing Calls* (Mar. 27, 2020), <https://www.ftc.gov/news-events/press-releases/2020/03/ftc-warns-nine-voip-service-providers-other-companies-against>.

<sup>46</sup> FTC Press Release, *FTC and FCC Sent Joint Letters to Additional VoIP Providers Warning against 'Routing and Transmitting' Illegal Coronavirus-related Robocalls* (May 20, 2020), <https://www.ftc.gov/news-events/press-releases/2020/05/ftc-fcc-send-joint-letters-additional-voip-providers-warning>; FTC Press Release, *FTC and FCC Send Joint Letters to VoIP Service Providers Warning against 'Routing and Transmitting' Illegal Coronavirus-related Robocalls* (Apr. 3, 2020), <https://www.ftc.gov/news-events/press-releases/2020/04/ftc-fcc-send-joint-letters-voip-service-providers-warning-against>.

<sup>47</sup> While there were likely many factors—including more aggressive blocking by phone companies and warning letters from the FTC and others—the FTC has seen a sharp drop in the number of robocall complaints since bringing a case against a large VoIP provider for facilitating illegal robocalls in December 2019. See FTC Press Release, *Court Halts Operations of VoIP Service Provider after the FTC and Ohio Alleged that It Helped Promote Credit Card Interest Reduction Scheme* (Dec. 5, 2019), <https://www.ftc.gov/news-events/press-releases/2019/12/court-halts-operations-voip-service-provider-after-ftc-ohio>.

<sup>48</sup> One AARP tele-town hall that the FTC participated in received more than 852,000 views just 4 days after posting the video. See AARP, *AARP's March 19 Coronavirus Tele-Town Hall* (Mar. 21, 2020), <https://www.aarp.org/podcasts/take-on-today/info-2020/coronavirus-town-hall-3-20.html>.

<sup>49</sup> FTC Consumer Alert, *Coronavirus scammers follow headlines* (Feb. 10, 2020), <https://www.consumer.ftc.gov/blog/2020/02/coronavirus-scammers-follow-headlines>.

<sup>50</sup> See [ftc.gov/coronavirus](https://www.ftc.gov/coronavirus).

<sup>51</sup> For example, the FTC issued a consumer alert following reports that nursing homes and assisted living facilities were illegally taking residents' stimulus payments. See FTC Consumer Alert, *Did a nursing home or assisted living facility take your stimulus check?* (May 15, 2020), <https://www.consumer.ftc.gov/blog/2020/05/did-nursing-home-or-assisted-living-facility-take-your-stimulus-check>.

<sup>52</sup> A pdf of the infographic can be downloaded here: [https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/keep\\_calm\\_infographic\\_en\\_508.pdf](https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/keep_calm_infographic_en_508.pdf).

<sup>53</sup> Moreover, the FTC's COVID-related blog post about fake checks from the government has received over 1.5 million views. See FTC Consumer Alert, *Checks from the government* (Mar. 18, 2020), <https://www.consumer.ftc.gov/blog/2020/03/checks-government>.

of Congress—to access, use, and share. In addition to our own social media activity, we encourage consumers to share the materials through social media and organizations to co-brand our materials and share them with their audiences.<sup>54</sup>

The FTC also has provided outreach specifically on privacy during the coronavirus pandemic, a concern of many businesses and consumers as the pandemic has shifted the workplace from traditional office spaces to consumers' homes. For example, the FTC has provided privacy and online security tips to consumers and businesses who have transitioned from working at an office to working from home.<sup>55</sup> The FTC also has provided information on contract tracing so that consumers do not divulge their sensitive personal information (such as financial information) to fake contract tracers, while emphasizing the importance of cooperating with legitimate contact tracers.<sup>56</sup> The pandemic has led to an increased reliance on technology to stay connected, and the Commission is staying abreast of privacy or data security issues that may arise so that consumers and businesses can better protect themselves in this increasingly virtual world.<sup>57</sup>

### VIII. CONCLUSION

The Commission appreciates Congress's confidence in the FTC's ability to protect consumers, especially with the unique challenges presented by the current COVID-19 pandemic. Through our enforcement, education, and policy efforts, we will continue to ensure that your confidence is well placed. We look forward to continuing to work with the Subcommittee and Congress.

Senator MORAN. Thank you very much, Mr. Smith.

Now Mr. Stu Sjouwerman, Founder and Chief Executive Officer, KnowBe4, Inc.

### STATEMENT OF STU SJOUWERMAN, FOUNDER AND CHIEF EXECUTIVE OFFICER, KNOWBE4, INC.

Mr. SJOUWERMAN. Mr. Chairman and members of the Committee, thank you for the opportunity to provide my perspective as Congress works toward developing solutions for businesses and governments combating COVID-19-related scams, and what more can be done to protect the public.

My name is Stu Sjouwerman. I am the Founder and CEO of KnowBe4, Inc. We are headquartered in Tampa Bay, Florida, with offices in Europe, South America, Australia, and Southeast Asia.

KnowBe4 is the provider of the world's largest security awareness training and simulated phishing platform. Our services are used by more than 33,000 organizations, with 24 million employees around the globe. And, for the last 30 years, I have served as an entrepreneur and data security expert in the IT industry.

I founded an anti-malware company called Sunbelt Software, which got multiple Inc. 500 awards and was acquired in 2010. And, as I was running that company, I realized that the human element of security was being seriously neglected, so I decided to help organizations to manage the ongoing problem of cybercrimes, social engineering tactics. And that is why I founded KnowBe4, to provide new school security awareness training. More than 33,000 organi-

<sup>54</sup> Various national organizations, including the National Association for the Advancement of Colored People, have worked with the FTC to co-brand COVID-19 scam infographics.

<sup>55</sup> FTC Business Alert, *Video Conferencing: 10 privacy tips for our business* (Apr. 16, 2020), <https://www.ftc.gov/news-events/blogs/business-blog/2020/04/video-conferencing-10-privacy-tips-your-business>; FTC Consumer Alert, *Online security tips for working from home* (Mar. 18, 2020), <https://www.consumer.ftc.gov/blog/2020/03/online-security-tips-working-home>.

<sup>56</sup> FTC Consumer Alert, *Help COVID-19 contract tracers, not scammers* (June 25, 2020), <https://www.consumer.ftc.gov/blog/2020/06/help-covid-19-contact-tracers-not-scammers>; FTC Consumer Alert, *COVID-19 contact tracing text message scams* (May 19, 2020), <https://www.consumer.ftc.gov/blog/2020/05/covid-19-contact-tracing-text-message-scams>.

<sup>57</sup> See also FTC Business Alert, *COPPA Guidance for Ed Tech Companies and Schools during the Coronavirus* (Apr. 9, 2020), [https://www.ftc.gov/news-events/blogs/business-blog/2020/04/coppa-guidance-ed-tech-companies-schools-during-coronavirus?utm\\_source=govdelivery](https://www.ftc.gov/news-events/blogs/business-blog/2020/04/coppa-guidance-ed-tech-companies-schools-during-coronavirus?utm_source=govdelivery).

zations in a variety of industries, including highly regulated fields such as healthcare, finance, energy, government, and insurance, have mobilized their end users as their last line of defense using KnowBe4.

Our primary objective is to enable employees—and they are also, of course, consumers—to make smarter security decisions by training them to become a human firewall in defense against social engineering attacks, which are responsible for upwards of 90 percent of data breaches.

The shutdowns and economic turmoil of the coronavirus pandemic have expanded the cyberattack surface, making it even easier for hackers and scammers to do their nefarious acts. If we don't focus on the human elements, consumers and employees, we ignore a crucial part of cybersecurity.

So, since the beginning of this year, COVID-19 has quickly reshaped the cyber threat landscape. For instance, over 192 coronavirus-related phishing attacks have occurred per week over the last month. No one is immune to being scammed, and different types of scams target different sets of consumers.

Scammers go to great lengths to make their attacks as convincing as possible, and many of these scams have very few visible signs that could tip off the recipients. The best way to fight scammers is to, of course, prevent, educate consumers and employees with a combination of security awareness training and frequent social engineering testing.

Here's one example. New data from security vendor Tripwire highlights how the shift to remote working has changed the face of cybersecurity for both current and future work climates. According to their report, 94 percent of organizations are more concerned about cybersecurity than before COVID-19. And they should be. The fact is that people are clicking on simulated COVID-19 phishing attacks at higher rates, and coronavirus-themed e-mails are rampant.

The emphasis in cybersecurity has traditionally been on hardware and software. However, we cannot solely rely on that. This strategy can't catch everything, nor does it address the need for a human firewall.

So, to end off, any support from Congress that would direct government agencies to implement ongoing security awareness training, more than just annual training that is typically in place, and include frequent social engineering testing would be greatly beneficial as we work together to bridge the gap in cybersecurity and protect American networks.

So, thank you for the opportunity to share KnowBe4's perspective on cybersecurity and our industry's unique ability to protect American citizens from rising COVID-19-related social engineering scams. We're grateful to Chairman Moran and the members of the Committee for the time and effort you are all putting into this important matter of national security. KnowBe4 is committed to being a helpful partner, going forward, as we all work to serve the best interest of the public.

Thank you.

[The prepared statement of Mr. Sjouwerman follows:]

PREPARED STATEMENT OF STU SJOUWERMAN, FOUNDER AND CHIEF EXECUTIVE  
OFFICER, KNOWBE4, INC.

Mr. Chairman and members of the committee, thank you for the opportunity to provide my perspective as Congress works towards developing solutions for businesses and governments combatting COVID-19 related scams and what more can be done to protect the public.

My name is Stu Sjouwerman, and I am the founder and Chief Executive Officer of KnowBe4, Inc., headquartered in Tampa Bay, FL with offices in Europe, South America, Australia and South East Asia.

KnowBe4 is the provider of the world's largest security awareness training and simulated phishing platform. Our services are used by more than 33,000 organizations around the globe. For the last 30 years, I have served as an entrepreneur and data security expert in the IT industry, and co-founded the Inc. 500 company Sunbelt Software, which was a multiple award-winning anti-malware software company that was acquired in 2010.

Realizing that the human element of security was being seriously neglected, I decided to help organizations manage the problem of cybercrime's social engineering tactics through new school security awareness training which is why I founded KnowBe4.

More than 33,000 organizations in a variety of industries—including highly-regulated fields such as healthcare, finance, energy, government and insurance—have mobilized their end users as their last line of cyber defense using KnowBe4.

KnowBe4 is founder-led and mission-driven. Our primary objective is to enable employees to make smarter security decisions by training them to become a "human firewall" in defense against social engineering attacks, which are responsible for upwards of 93 percent of data breaches.

The shutdowns and economic turmoil of the coronavirus pandemic have expanded the cyber attack surface, making it even easier for hackers and scammers. Ransomware and malware attacks are up, and users working from home are more susceptible to phishing attempts and other social engineering tactics to gain access to networks. If we don't focus on the human element—consumers and employees—we ignore a crucial part of cyber security.

Covid-19 has quickly reshaped the cyber threat landscape. For example, over 192,000 coronavirus-related phishing attacks have occurred per week over the last month. No one is immune to being scammed, and different types of scams target different sets of consumers. Scammers go to great lengths to make their attacks as convincing as possible, and many of these scams have very few visible signs that could tip off recipients. Consumers should not assume they can spot every scam attempt, and that bias only helps the scammers. The best way to fight scammers is educating consumers and employees with a combination of security awareness training and frequent social engineering testing.

New data from security vendor Tripwire highlights how the shift to remote working has changed the face of cybersecurity for both the current and future work climate. According to their report, 94 percent of organizations are more concerned about cybersecurity than before COVID-19—and they should be. The fact is, people are clicking on simulated COVID-19 phishing attacks at high rates and Coronavirus themed e-mails are rampant.

Malicious actors are aggressively exploiting the COVID-19 crisis by re-purposing and overhauling the phishing e-mails they were running before the Coronavirus emerged in late December. Although the bad guys have been developing new social engineering schemes uniquely based on the onslaught of recent events, these COVID-19 "re-treads" are fast becoming the most common variety of Coronavirus-themed phishing e-mails that we encounter on a day-to-day basis.

It's no surprise that phishers and scammers are using the avalanche of new information and events involving the global coronavirus pandemic as a way to successfully phish more victims. These phishing scams are becoming more aggressive and more targeted as this pandemic continues. COVID-19 phishers prey on both consumers and employees and have sought private information through targeting passport details, the healthcare industry, social media channels, and we can expect to see them use current and future COVID-19 lawsuits as bait in spear phishing attacks. Everyone should remain very skeptical of any e-mail related to COVID-19 coming into their inbox.

The emphasis in cybersecurity has traditionally been on hardware and software. However, we cannot solely rely on that. This strategy cannot catch everything, nor does it address the need for a human firewall. The largest breaches in our country—to include John Podesta's personal e-mail, our U.S. power grid, JP Morgan Chase,

Sony Pictures, etc.,—these systems relied on hardware and software for defense, yet still fell victim to phishing attacks.

Through new-school security awareness training, the likelihood of such social engineering attacks are significantly decreased, and organizations are inoculated against the types of compromises we’re seeing today.

Any support from Congress that would direct government agencies to implement *ongoing* security awareness training—more than the annual training typically in place—and include frequent social engineering testing would be greatly beneficial as we work together to bridge the gap in cyber security and protect American networks.

Thank you for the opportunity to share KnowBe4’s perspective on cybersecurity and our industry’s unique ability to protect American citizens from rising COVID-19 related social engineering scams. We are grateful to Chairman Moran and the members of the committee for the time and effort you all are putting into this important matter of national security. KnowBe4 is committed to being a helpful partner going forward as we all work to serve the best interest of the public.

Senator MORAN. Thank you very, very much.

Now Ms. Laura MacCleery, Policy Director, Center for Science in the Public Interest.

Welcome.

**STATEMENT OF LAURA MACCLEERY, POLICY DIRECTOR,  
CENTER FOR SCIENCE IN THE PUBLIC INTEREST**

Ms. MACCLEERY. Thank you, Chairman Moran and Ranking Member Blumenthal, for the honor of testifying today on this critical topic.

I am Policy Director for Center for Science in the Public Interest, a nearly 50-year-old organization that works to improve the health of the food supply and the interests of consumers.

Americans are facing an unprecedented challenge in keeping themselves and their families safe during a pandemic. Public health officials emphasize that we all need to socially distance, wear a mask, and wash our hands. Understandably, though, many people are looking for more to protect themselves, and those without scruples are actively exploiting consumer fear and anxiety.

In truth, our under-regulated marketplace for dietary supplements is a risky place under any conditions. For the past 3 years, we’ve been collecting evidence of scams concerning supplements, and sending it to the Food and Drug Administration and the Federal Trade Commission. These included many misleading claims we found on products marketed to vulnerable consumers suffering from opioid and tobacco addiction, as well as supplements making false claims on female fertility.

It is far too tempting to think that a powder or a supplement can help us with a global pandemic. When the coronavirus appeared, we knew the hucksters would not be far behind.

First, we wrote the FDA and FTC about televangelist Jim Bakker, whom we heard Senator Blumenthal describe. That show featured experts advancing the claim that the products it sold containing colloidal silver could cure coronavirus, quote, “within 12 hours.” The commentators on the same show had previously claimed that the same product cures, quote, “all venereal diseases as well as HIV.” Yet, there’s no evidence that silver supplements prevent or treat any condition, according to the National Institutes of Health. Although experts featured on the show claimed that it could be consumed daily, in “slurps,” and was, quote, “safe for ba-

bies,” colloidal silver in large enough amounts can be dangerous to kidneys and other organs. It can also cause permanent bluish-gray discoloration of a person’s skin and organs.

Also in June, we sent another request to the FDA and FTC asking for enforcement on supplements being marketed as antiviral claims. Any claim that a supplement has antiviral properties is considered an illegal disease claim by the FDA, because only drugs can cure or treat disease.

Our market scan of products on Amazon in late May found 46 dietary supplements making illegal antiviral claims, so we wrote the agencies and Amazon directly for removal. Unfortunately, a subsequent search of Amazon performed on June 29 found that 26 of these—those supplements are still making antiviral claims on their own websites, on Amazon, or other online stores.

We continue to be on the lookout for scams related to COVID claims. Just this morning, we sent public letters to the FDA and FTC asking for the agencies to act to address dozens of misleading claims made by about 23 supplements and medical devices by Dr. Joseph Mercola, a well-known purveyor of dietary supplements.

In a pandemic, such untruths pose a clear and urgent danger. Consumers may develop a false sense of security and fail to practice social distancing or use masks, endangering themselves or everyone around them. They also may harm themselves by taking dangerous doses of supplements or fail to seek effective medical treatment, believing, instead, in the promises of charlatans. But, it’s even worse than that. On a recent episode of Mercola’s podcast, he actually advises consumers to take the immunity-boosting supplements he sells and then deliberately attempt to contract COVID-19 because his supplements will allegedly reduce their symptoms.

Dietary supplements are, in fact, among the most poorly regulated consumer products. Congress, through the Dietary Supplement Health and Education Act of 1994, established a bare-bones system of oversight that was designed to be weak. Today, particularly given the tremendous expansion of products and use by consumers over the past 26 years, that system is failing.

Both the FDA and the FTC need more funding, personnel, and resources for enforcement. The FDA, in particular, needs far better tools, including a mandatory product registration requirement, to make the marketplace transparent for regulators and consumers. In addition, Congress should authorize State Attorneys General to enforce relevant Federal laws related to dietary supplements to improve their accountability and reach. And the FDA should be given heightened regulatory powers for specific categories of supplements that are known to pose a high risk to consumers because they are marketed to vulnerable groups or are commonly tainted with drugs and synthetic ingredients.

We would appreciate the opportunity to work with lawmakers on a vision for reform of supplement oversight to ensure that consumers are protected from fraud. It should not take a pandemic to motivate solutions to require that supplements, like any consumer product, are truthfully labeled and marketed, and that consumers are not misled in ways that risk their own and public health.

Thank you. And I’m happy to answer any questions.

[The prepared statement of Ms. MacCleery follows:]

PREPARED STATEMENT OF LAURA MACCLEERY, POLICY DIRECTOR, CENTER FOR  
SCIENCE IN THE PUBLIC INTEREST

Thank you, Chairman Moran and Ranking Member Blumenthal for the honor of testifying today on this critical topic. I am the Policy Director for the Center for Science in the Public Interest, a nearly fifty-year-old organization that advocates for healthy changes to our food system and for the interests of consumers.

Americans are facing an unprecedented challenge in keeping themselves and their families safe during a pandemic. Public health officials emphasize that we all need to socially distance, wear a mask, and wash our hands. But understandably, many people are looking for more than those measures to protect themselves, and those who lack scruples are actively exploiting consumer fear and anxiety.

In truth, our underregulated marketplace for dietary supplements is a risky place under any conditions. For the past three years, we have been collecting evidence of scams concerning supplements and sending it to the Food and Drug Administration (FDA) and Federal Trade Commission (FTC). These have included the many misleading claims we found on products marketed to vulnerable consumers suffering from opioid<sup>1</sup> and tobacco addiction.<sup>2</sup>

Last November, we reported to the agencies about 39 supplements selling false hope to women experiencing infertility by making unsupported disease claims, a practice precluded by law.<sup>3</sup> Only products approved as drugs may make claims to treat or prevent a disease or health condition, such as infertility or the coronavirus.

It is far too tempting to think that a powder or supplement can help us against a global pandemic. When the coronavirus appeared, we knew the hucksters would not be far behind. We have been tracking and reporting such efforts to appropriate Federal authorities since February.

First, we wrote the FDA and FTC about televangelist Jim Bakker, whose show featured experts advancing the claim that products it sold containing colloidal silver could cure the coronavirus “within 12 hours.”<sup>4</sup> Commentators on the same show previously claimed that the same product cures “all venereal diseases,” as well as HIV.<sup>5</sup>

Yet there’s no evidence that silver supplements prevent or treat any condition, according to the National Institutes of Health.<sup>6</sup> Although experts featured on Bakker show claimed it should be consumed daily in “slurps” and was “safe for babies,”<sup>7</sup> colloidal silver in large enough amounts can be dangerous to kidneys and other organs.<sup>8</sup> It can also cause permanent bluish-gray discoloration of a person’s skin and organs.<sup>9</sup>

<sup>1</sup> Center for Science in the Public Interest (CSPI). *Crackdown Urged on Supplements Marketed as Opioid Withdrawal Aids: CSPI Investigation Shows Manufacturers Can’t Support Claims*. December 8, 2017. <https://cspinet.org/news/crackdown-urged-supplements-marketed-opioid-withdrawal-aids-20171208>. Accessed July 16, 2020.

<sup>2</sup> CSPI. *FDA Urged to Take Enforcement Action against Manufacturers of Dietary Supplements that Promise to Help Smokers Quit: Companies Produce No Evidence to Support their Claims*. April 23, 2019. <https://cspinet.org/news/fda-letter-dietary-supplements-smoking-cessation>. Accessed July 16, 2020.

<sup>3</sup> CSPI. *Manufacturers of “Fertility” Supplements Selling False Hope: CSPI Asks the FDA and FTC to Take Enforcement Action*. November 15, 2019. <https://cspinet.org/news/manufacturers-fertility-supplements-false-hope-20191118>. Accessed July 16, 2020.

<sup>4</sup> CSPI. *CSPI Urges FDA Enforcement Action on Televangelist Jim Bakker’s Fake Coronavirus “Cure”: Letter Submitted to FDA and FTC*. February 20, 2020. <https://cspinet.org/news/cspi-urges-fda-enforcement-action-televangelist-jim-bakkers-fake-coronavirus-cure-20200218>. Accessed July 16, 2020.

<sup>5</sup> *Id.*; Right Wing Watch Twitter Page (@RightWingWatch). February 12, 2020 (1:17pm). [https://twitter.com/RightWingWatch/status/1227657884395327489?ref\\_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwtterm%5E1227657884395327489&ref\\_url=https%3A%2F%2Fwww.lgbtqnation.com%2F2020%2F02%2Ftelevangelist-jim-bakker-claims-silver-solution-std-cure-also-kills-coronavirus%2F](https://twitter.com/RightWingWatch/status/1227657884395327489?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwtterm%5E1227657884395327489&ref_url=https%3A%2F%2Fwww.lgbtqnation.com%2F2020%2F02%2Ftelevangelist-jim-bakker-claims-silver-solution-std-cure-also-kills-coronavirus%2F). Accessed July 16, 2020.

<sup>6</sup> Mayo Clinic. *My dad takes colloidal silver for his health, but is it safe?*. September 6, 2017. <https://www.mayoclinic.org/healthy-lifestyle/consumer-health/expert-answers/colloidal-silver/faq-20058061>. Accessed July 16, 2020.

<sup>7</sup> CSPI. *CSPI Urges FDA Enforcement Action on Televangelist Jim Bakker’s Fake Coronavirus “Cure”: Letter Submitted to FDA and FTC*. February 20, 2020. <https://cspinet.org/news/cspi-urges-fda-enforcement-action-televangelist-jim-bakkers-fake-coronavirus-cure-20200218>. Accessed July 16, 2020.

<sup>8</sup> National Center for Complementary and Integrative Health. *Colloidal Silver*. April 2017. <https://nccih.nih.gov/health/colloidalsilver>. Accessed July 16, 2020.

<sup>9</sup> *Id.*

The FDA and FTC issued warning letters to The Jim Bakker Show,<sup>10</sup> as did the New York<sup>11</sup> and Missouri Attorneys General,<sup>12</sup> and the religious group Faithful America is asking for networks to drop the show because of these statements.<sup>13</sup> In June, the Arkansas Attorney General brought a civil claim against the show, seeking compensation for consumers.<sup>14</sup>

Also in June, we sent another request to the FDA and FTC, asking for enforcement on supplements being marketed as “antiviral” products.<sup>15</sup> Any claim that a supplement has antiviral properties is considered an illegal disease claim by the FDA because viruses are, obviously, a form of disease.<sup>16</sup>

Our market scan of products on Amazon in late May found at least 46 dietary supplements making illegal antiviral claims, so we sent our findings to the agencies and wrote Amazon directly to ask the company to remove these products.<sup>17</sup> Unfortunately, a subsequent search of Amazon performed on June 29th found that 26 of those supplements are still making antiviral claims on their own websites, Amazon, or other online stores.

While Amazon has already rid its site of many products bearing explicitly illegal COVID claims,<sup>18</sup> others have done little. Because consumers rely on them so much today, platforms such as Amazon, Ebay, Facebook and Etsy must do a far better job of removing misleading claims and products being sold and marketed through their sites, and we urge Congress and the agencies to hold them accountable for doing so.

We continue to be on the look-out for scams related to COVID claims. Just this morning, we sent public letters to the FDA and FTC asking for the agencies to act to address dozens of misleading claims made about at least 23 supplements and medical devices by Dr. Joseph Mercola, a well-known purveyor of dietary supplements over the Internet.

According to Dr. Mercola and his companies’ website, Mercola.com, it is the world’s “#1 most visited natural health website” and is viewed by “millions of people

<sup>10</sup>U.S. Food and Drug Administration (FDA). *WARNING LETTER: The Jim Bakker Show MARCS-CMS 604820*. March 06, 2020. <https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/warning-letters/jim-bakker-show-604820-03062020>. Accessed July 16, 2020.

<sup>11</sup>State of New York, Office of the Attorney General. *Letter RE: CEASE AND DESIST NOTIFICATION*. March 3, 2020. [https://ag.ny.gov/sites/default/files/bakker\\_cease\\_and\\_desist\\_letter\\_notification.pdf](https://ag.ny.gov/sites/default/files/bakker_cease_and_desist_letter_notification.pdf). Accessed July 16, 2020.

<sup>12</sup>Missouri State Attorney General. *AG Schmitt Files Suit Against Jim Bakker for Selling Fake “Coronavirus Cure”*. Mar 10, 2020. <https://ago.mo.gov/home/news/2020/03/10/ag-schmitt-files-suit-against-jim-bakker-for-selling-fake-coronavirus-cure>. Accessed July 16, 2020.

<sup>13</sup>Faithful American. *Tell DirecTV, DISH, and Roku: Drop televangelist for selling fake coronavirus cure*. March 7, 2020. <https://act.faithfulamerica.org/sign/bakker-coronavirus/>. Accessed July 16, 2020.

<sup>14</sup>Arkansas Attorney General. *Rutledge Sues Jim Bakker for Peddling Colloidal Silver Products to Cure COVID-19*. June 16, 2020. <https://arkansasag.gov/media-center/news-releases/rutledge-sues-jim-bakker-for-peddling-colloidal-silver-products-to-cure-covid-19>. Accessed July 16, 2020.

<sup>15</sup>CSPI. *CSPI Letters re: Antiviral Claims by Supplement Manufacturers: Sent to FDA, FTC, Amazon*. June 3, 2020. <https://cspinet.org/resource/cspi-letters-re-antiviral-claims-supplement-manufacturers>. Accessed July 17, 2020.

<sup>16</sup>Agency guidance provides that: “A claim that a dietary supplement fights disease or enhances disease-fighting functions of the body is a disease claim. Under this criterion, context and specificity are important. Claims such as ‘supports the body’s ability to resist infection’ and ‘supports the body’s antiviral capabilities’ are disease claims because the context of the claim is limited to the disease prevention and treatment capabilities.” FDA. *Small Entity Compliance Guide on Structure/Function Claims*. January 9, 2002. <https://www.fda.gov/regulatory-information/search-fda-guidance-documents/small-entity-compliance-guide-structurefunction-claims>. Accessed May 4, 2020.

<sup>17</sup>CSPI. *CSPI Letters re: Antiviral Claims by Supplement Manufacturers: Sent to FDA, FTC, Amazon*. June 3, 2020. <https://cspinet.org/resource/cspi-letters-re-antiviral-claims-supplement-manufacturers>. Accessed July 17, 2020.

<sup>18</sup>U.S. Immigration and Custom Enforcement (ICE). *HSI partners with Pfizer, 3M, Citi, Alibaba, Amazon, Merck to protect consumers against COVID-19-related fraud*. May 5, 2020. <https://www.ice.gov/news/releases/hsi-partners-pfizer-3m-citi-alibaba-amazon-merck-protect-consumers-against-covid-19>. Accessed May 6, 2020. (“Since the beginning of the COVID-19 crisis, Amazon has proactively stopped more than 6.5 million products with inaccurate claims, removed over 1 million offers for suspected price gouging, suspended more than 10,000 selling accounts for suspected price gouging and referred the most egregious offenders to Federal and state law enforcement across the country. Amazon welcomes HSI’s partnership in holding counterfeiters and bad actors accountable, and we look forward to building on our long-standing relationship to protect customers and ensure a trusted shopping experience,” said Dharmesh Mehta, Amazon vice president, customer trust and partner support.”).

daily.”<sup>19</sup> Working with Justice Catalyst Law,<sup>20</sup> and People’s Parity Project,<sup>21</sup> we documented how he markets these supplements and devices by falsely claiming that they will protect people from, or treat symptoms of, COVID-19.<sup>22</sup>

In a pandemic, such untruths pose a clear and urgent danger. Consumers may develop a false sense of security and fail to practice social distancing or use masks, endangering themselves and everyone around them. They may also harm themselves by taking dangerous doses of supplements, or fail to seek effective medical treatment, believing instead in the promises of charlatans.

But it is even worse than that. On a recent episode of Mercola’s podcast, he actually advises consumers to take the immunity-boosting supplements he sells and then attempt to contract the COVID-19 virus deliberately, because his supplements will allegedly reduce their symptoms.<sup>23</sup> Even with all my experience investigating supplement scams, this reckless self-promotion and endangerment of the public took my breath away.

Such potentially deadly advice to consumers, and the profiteering from our legitimate fears, must be stopped. While the agencies are working hard to stem the tide of misleading products, the funding and enforcement tools they currently have are woefully inadequate to this task.

Dietary supplements are among the most poorly regulated consumer products. Congress, through the Dietary Supplement Health and Education Act of 1994 (DSHEA), established a bare-bones system of oversight by the Food and Drug Administration (FDA) that was designed to be weak. Today, particularly given the tremendous expansion of products and use by consumers over the intervening 26 years, that system is indisputably failing.

Both the FDA and FTC need more funding, personnel and resources for enforcement. The FDA, in particular, needs far better tools, including a mandatory product registration requirement to make the marketplace transparent for regulators. A modest and graduated registration fee could also be collected to build resources at the agency.

In addition, Congress should authorize state attorneys general to enforce relevant Federal laws related to dietary supplements, to improve their accountability and

<sup>19</sup> See Dr. Joseph Mercola (Mercola). *Health Website Rankings: Mercola.com is World’s Most Visited Natural Health Site*. <https://www.mercola.com/forms/rankings.htm>. Accessed July 16, 2020.

<sup>20</sup> Justice Catalyst Law (JCL) is a nonprofit law firm that focuses on combatting social and economic injustice, working nationally to support cases and policy work in the fields of antitrust, consumer law, employment law and civil rights. See, <https://justicecatalyst.org>. Accessed July 16, 2020.

<sup>21</sup> People’s Parity Project (PPP) organizes law students and new attorneys nationwide to unrig the legal system and build a justice system that values people over profits. PPP believes that by dismantling the coercive legal tools that enhance corporate power and fighting for a judiciary that is representative of—and thus responsive to—people, not corporations, can reshape the legal profession. See, <https://www.peoplesparity.org>. Accessed July 16, 2020.

<sup>22</sup> Such products, sold through its online store, and that Dr. Mercola has endorsed in public statements (See *supra* note 23) for the prevention and/or treatment of COVID-19, include: vitamin C (specifically, liposomal vitamin C); vitamin D; zinc and selenium (which Mercola Group sells together); melatonin; licorice; molecular hydrogen; astaxanthin; n-acetyl cysteine; prebiotics, probiotics, and sporebiotics; saunas; ozone therapy; elderberry extract; spirulina; beta-glucan; lipoic acid; and sulforaphane. See, e.g., Mercola, *Nutrition and Natural Strategies Offer Hope Against COVID-19*, Mar. 29, 2020. <https://articles.mercola.com/sites/articles/archive/2020/03/29/andrew-saul-vitamin-c.aspx>. Accessed July 16, 2020; Mercola, *Coronavirus Resource Page*. <https://www.mercola.com/coronavirus-resources.htm>. Accessed July 16, 2020; Mercola and Andrew Saul, *Nutrition and Natural Strategies Offer Hope Against COVID-19: Discussion Between Drs. Andrew Saul and Mercola*, Dr. Joseph Mercola—Take Control of Your Health. Mar. 29, 2020. <https://podcasts.apple.com/us/podcast/nutrition-natural-strategies-offer-hope-against-covid/id1286870871?i=1000469858840>. Accessed July 16, 2020; <http://Shop.Mercola.com>. Accessed July 16, 2020; <https://bit.ly/2XBFJ9d> (Liposomal Vitamin C). Accessed July 16, 2020; <https://bit.ly/372lcxy> (Liposomal Vitamin D3). Accessed July 16, 2020; <https://bit.ly/2UbOKmX> (Molecular Hydrogen). Accessed July 16, 2020; <https://bit.ly/3gYhxx5> (Melatonin). Accessed July 16, 2020; <https://bit.ly/2UeDlmJ> (Zinc plus Selenium). Accessed July 16, 2020; <https://bit.ly/3758gqA> (Ozone generating air purifiers). Accessed July 16, 2020; <https://bit.ly/3dDEOpk> (Infrared Saunas—temporarily discontinued for “redesign”). Accessed July 16, 2020.

<sup>23</sup> Mercola stated: “When you get a vaccine, you only simulate your humoral immunity, the B-cells. The T-cells are not stimulated. So, scary as it may sound, the best thing is to get the infection, and have a strong immune system to defend against it so you won’t even display any symptoms.” Here, Dr. Mercola made the misleading and false assertion that contracting the virus and recovering will confer a “natural immunity” that will be more effective than the immunity provided by a vaccine. Mercola and Andrew Saul, *Nutrition and Natural Strategies Offer Hope Against COVID-19: Discussion Between Drs. Andrew Saul and Mercola*, Dr. Joseph Mercola—Take Control of Your Health. Mar. 29, 2020. <https://podcasts.apple.com/us/podcast/nutrition-natural-strategies-offer-hope-against-covid/id1286870871?i=1000469858840>. Accessed July 16, 2020.

reach. Currently, state AGs can only enforce general consumer protection laws under their own state regime, not Federal rules on supplements. Yet the sheer number of products make it practically impossible for one central agency to monitor and enforce compliance with legal requirements.

The FDA should also be given heightened regulatory powers for specific categories of supplements known to pose a “high risk” to consumers because they are marketed to vulnerable groups or are commonly tainted with drugs or synthetic ingredients. Many such products—including sexual-enhancement, weight-loss, and workout supplements—are already identified as high risk because agency testing reveals they often contain drugs such as amphetamines.<sup>24</sup>

These and other categories of high-risk supplements should be subjected to pre-market product testing and audits in a new, focused safety program authorized and funded by Congress. Ironically, under current law, because these are tainted with drugs, they are not subject to mandatory recall—a loophole that should be closed.<sup>25</sup> There are other needs as well:

- Companies should be required to report all adverse events that result from their products, not merely the ones they deem “serious.”
- Supplements that interact with common categories of prescription drugs should bear a warning for consumers about the risk of an interaction.
- A loophole that allows new supplements to side-step safety review should be closed.<sup>26</sup> A leading trade association representative admitted at a 2018 FDA public meeting that the industry uses this loophole “six to seven times” more than the official safety approval process they are supposed to use under the law, thereby avoiding any review for safety at all.<sup>27</sup>
- Last, rules that have languished unfinished since 1994, including defining what a “new dietary ingredient” is, should be completed by the FDA, and Congress should set deadlines for that completion.<sup>28</sup>

We would appreciate the opportunity to work with lawmakers on a vision for reform of supplement oversight to ensure that consumers are protected from fraud. It should not take a pandemic to motivate solutions to require that supplements—like any consumer product—are truthfully labeled and marketed, and that consumers are not misled in ways that risk their own and public health.

Senator MORAN. Thank you very much for your presence and testimony.

Let me begin with a question, initially for Mr. Smith. On April the 14th, Senator Blumenthal and I sent a letter to FTC Chairman Joseph Simons asking if the FTC currently had the authority, under its relatively flexible Section 5 authority, to enforce against unfair and deceptive acts or practices to deal with the issue of price gouging.

On May 19, the Chairman responded, indicating there are significant legal challenges under our current statutory authority to

<sup>24</sup>FDA. *Tainted Dietary Supplements and Foods: Responsibilities of Retailers and Distributors*. October 2010. <https://www.fda.gov/files/drugs/published/Tainted-Dietary-Supplements-and-Foods-Responsibilities-of-Retailers-and-Distributors.pdf>. Accessed July 16, 2020.

<sup>25</sup>Such a provision would state that if a product is sold as a dietary supplement and contains an ingredient approved by the FDA for use as a prescription drug, FDA may initiate a recall of the product.

<sup>26</sup>The Dietary Supplement Health and Education Act of 1994 (DSHEA) requires companies that introduce novel substances into dietary supplements provide the FDA with information showing that the “new dietary ingredients” (NDIs) in supplements will “reasonably be expected to be safe.” However, FDA draft guidance on NDIs has never been completed, and perhaps three-quarters or more of NDIs evade FDA’s review by following a pathway permitted for secret and unmonitored self-assessment by companies of the safety of ingredients in food, known as “Generally Recognized as Safe,” or “GRAS,” self-determination. See 21 U.S.C. § 350b; 62 Fed. Reg. 49886 (September 23, 1997), Premarket Notification for a New Ingredient.; See also CSPI *FDA Food Ingredient Approval Process Violates Law, Says CSPI: Flawed ‘GRAS’ System Lets Novel Chemicals Into Food Supply without FDA Safety Review*. April 15, 2015. <http://cspinet.org/new/201504151.html>. Accessed July 17, 2020.

<sup>27</sup>FDA. *Public Meeting to Discuss the Development of a List of Pre-DSHEA Dietary Ingredients*. P. 49. October 2017. Transcript available at <https://www.fda.gov/media/108452/download>. Accessed May 11, 2020.

<sup>28</sup>The FDA has yet to issue final draft guidance on how companies should show that the “new dietary ingredients” (NDIs) in supplements will “reasonably be expected to be safe.”

address price-gouging allegations, and that they rely heavily on the DOJ and State Attorneys General to enforce such activities.

Mr. Smith, historically the FTC has not used its Section 5 authority related to those unfair and deceptive acts or practices to take enforcement actions related to price gouging. If Congress were to legislate to explicitly direct the FTC to address price gouging, would you have recommendations for this subcommittee as to what that should look like?

Mr. SMITH. Right. So, you're right that historically the Commission has not—there have been these supply shocks, you know, following natural disasters and the like, and the Commission has been asked, you know, "Could the unfairness authority fit the increased prices that follow those supply shocks?" And the Commission has historically been reluctant to use its unfairness authority in that way.

I would note that, you know, at least 35 other states have UDAP authority, as well, similar to our unfairness authority, but have seen fit to enact price-gouging statutes, including Kansas—General Schmidt, in his written remarks, talked a bit about that—and the State of Connecticut and a lot of other states.

So, you know, we think that a special law would be helpful here. And, with respect to that law, what we have—and we've worked with some of your offices on this—what we would recommend is that the crisis to which the statute applies be clearly defined, and that it be truly national in scope, not one of these, you know, regional or local supply shocks that might call upon the national Federal Trade Commission to address those issues, so that there be—so there'd be a narrowly defined, or at least clearly defined, national crisis that a statute applies to; that it would be nice if it were to define the types of materials or products or services that would be covered—for example, PPE, in the current crisis; that there be a clearly defined trigger, such as an increase in price over a pre-crisis index—so, 25-percent increase in price, for example, is what some State laws account for; and also that there be some acknowledgment that increased costs might be legitimate. So, for example, if there's a disruption in the supply chain, and a merchant needs to find alternative supplies, and it results in increased costs, we don't want to discourage that. We want to encourage new entrants to the marketplace. We want to—you know, we don't want to discourage people from providing critical goods and services simply because their costs have increased.

So, I think that those three or four items that I've outlined would be really helpful in any national price-gouging legislation.

Senator MORAN. Thank you.

You mentioned the State of Kansas. Let me turn to the Attorney General.

General Schmidt, we do have a law in place, as you indicated and Mr. Smith indicated. Tell me, if you would, describe your office's efforts in enforcing that law, that State law.

Mr. SCHMIDT. Mr. Chairman, we do. After the 9/11 attacks, the State of Kansas enacted what is now known as our Profiteering from Disaster Statute, which, in the colloquial, would be our anti-price-gouging law.

The way it is structured is that it is in effect only during a time—and in the place, in the geographical area—of a declared state of emergency, either by our Governor or by the President. So, those are the two triggers that cause the law to enter into force. The standard is any unjustified increase of pricing, as compared with the price for a particular product or service on the day before the emergency was declared, and unjustified—there's a presumption that something was unjustified if it's 25-percent-or-more increase, although, if it's a passthrough cost, as Mr. Smith suggested, that's—that negates the presumption and also operates as a defense. And it applies to what the statute calls “necessary goods or services,” which are further defined as, essentially, things that consumers are likely to need more of as a result of the particular emergency. So, that's the structure of our statute.

To your question about our efforts to enforce it, it has been enforced—in effect now in Kansas longer and in a more widespread way than ever before, during the COVID response, because of the nature of the emergency. We have approached this—we've received—last I looked, it was somewhere around 400 complaints from Kansans alleging a violation of that statute. We've investigated them all. And—or are investigating them all—and, generally speaking, we've approached this through education or engagement with the supplier, with the retailer. A lot of times, we discover they didn't know that the law existed, because it's so rarely in effect. Other times, it's plain on its face that they're simply passing through costs that were raised for them, so we can then go up the supply chain to figure out if there's anything unlawful happening. So, we've tried to approach it in that way. We have not, at this point, had to actually file an enforcement action. We have had a number of suppliers change their behavior once we've engaged with them, however.

Senator MORAN. General, thank you.

I now turn to a former State Attorney General, the Ranking Member, Senator Blumenthal.

Senator BLUMENTHAL. Yes, I want to welcome you particularly, Attorney General Schmidt, and thank you for the good work you're doing out there. And I think you provide evidence as to one of the recommendations that Ms. MacCleery makes about the need for authority on the part of State Attorneys General to enforce Federal laws.

So, let me ask, if I may, Mr. Smith, what do you think about giving State Attorneys General broader authority?

Mr. SMITH. So, generally—so, I'm speaking just for myself—right?—not for the Commission or for any individual commissioner. A lot of the consumer protection laws in which—that we currently enforce have authority for State Attorneys General to enforce them, as well. And I think that's terrific, honestly. And it's a big help for us, I think, that, if the State Attorneys General are willing to share some of the load with respect to enforcement, we are delighted for that.

I would say that, typically, when there is a provision permitting State Attorney General enforcement, that the Federal Trade Commission, or whomever the relevant Federal authority might be, have an opportunity to get—one, that it receives notice of the case

before being filed, and that it has an opportunity to intervene. But, with those safeguards, I think that, you know, traditionally, we, at the Federal Trade Commission, have been in favor of State AG enforcement of the Federal statutes that we enforce.

Senator BLUMENTHAL. Ms. MacCleery, I want to thank you for the work that your organization does. The Center for Science in the Public Interest really does magnificent research and policy formulation. And I think what you've done on these fake and phony cures is show not only that there's a financial cost, but also that they have serious adverse side effects. And I don't mean only that the potential physical dangers, medically. I mean, the sense of false security that may cause complacency, a failure to practice good preventive action, like wearing masks and physical distancing and the kinds of dangers that they pose when people talk about them and exaggerate them to their friends or neighbors. So, I think there's a special responsibility on the part of everyone who is involved in promoting these products. And I note, in your testimony, that you make reference to Amazon, eBay, Facebook, and Etsy. And I'm quoting, "must do a better—must do a far better job of removing misleading claims and products." Shouldn't they be held accountable?

Ms. MACCLEERY. Yes. I think that there has been a perception that the third-party platforms are just a marketplace without a stake in the game. Increasingly, we see that that is not the right understanding of the model. They profit from having all the sellers on their platform. They learn tremendous amounts about the marketplace and the behavior of buyers and sellers. They often produce their own products, in the case of Amazon or Walmart (which has a big online presence), and sell them directly to sellers. And they should be asked to help patrol the viability of claims on the marketplaces that they're managing.

The antiviral complaints that we've filed have been very disappointing, because to see the lack of response, on the part of Amazon, to those. They are doing some coordination, is my understanding from news reports, with the Department of Homeland Security around COVID products that are specifically marketed to treat or prevent COVID, which is commendable. And what we'd like to do is see more of that sort of shared enforcement model.

Amazon has been found liable in court for selling foods that should have been recalled after they were identified by the CDC as having a food-borne pathogen. In addition, we were working with a family that lost their son to unwashed poppy seed tea, which is an opiate, and the seeds were sold through Amazon in bulk amounts to be used for this purpose. And it was clear, from the comments on this site, that these products were used for drug purposes.

So those are the kinds of things that we see. And we think that there could be a much more compelling partnership between the platforms and the government to deal with fraud and abuse.

Senator BLUMENTHAL. They could be much more aggressive. And don't they have an obligation to be more aggressive? If you search for "COVID cure" on Amazon, you still find sponsored banners for probiotics and product listings for supplement. Aren't they

complicit, along with other marketplaces? And have you been satisfied with their response to your complaints?

Ms. MACCLEERY. I think they have a tricky job controlling the algorithm, which might, in part, be learning from consumer practices in real time on their site, but I don't know enough about how the Amazon search engine works, because it's not very clear, from looking over the site protocols. So, that would be an area for investigation by Congress or the agencies, in consultation with the company.

I do think where we have flagged items, like the antiviral claims, which are *per se* illegal claims, according to the Food and Drug Administration, they have a clear obligation to act. And there are also supplements that are tainted with prescription drugs that have been sold through Amazon, and those need to be expeditiously removed as soon as the platforms are informed that they are tainted.

Senator BLUMENTHAL. Thank you.

My first round—I hope there will be a second round, Mr. Chairman—has expired, so I'll yield back and hope that we can ask more questions.

Senator MORAN. We'll follow our usual practice of not informing the other committee members whether there will be a second round or not until we see how many people are here.

[Laughter.]

Senator MORAN. The—we now turn to the Full Committee Chairman, who's certainly entitled to a second round.

Senator Wicker, thank you for joining us.

#### **STATEMENT OF HON. ROGER WICKER, U.S. SENATOR FROM MISSISSIPPI**

The CHAIRMAN. Well, thank you very much, Senator Moran. I appreciate the work that you and Senator Blumenthal are doing on this issue.

I have a prepared statement that I will ask be included in the record following the opening statement of Senator Blumenthal.

Senator MORAN. Without objection.

The CHAIRMAN. Thank you very much.

And I've very much enjoyed the testimony.

You know, Mr. Smith, we are looking, right now, in the House and Senate at a COVID-19 response bill, a Phase 4, and this is a good opportunity for, I think, us to see if you need anything in that bill.

Ms. MacCleery says that FTC does not have enough funding or enforcement tools to go after the scammers. And so—but, you haven't asked for any additional full-time equivalents. So, one thing I'd like for you to discuss is—you have enough resources to fulfill the task that we're talking about today, and then, with regard to—following up on Senator Blumenthal's question about State Attorneys General, maybe that's a way for us, indeed, to spread some of the responsibility, let the 50 Attorneys General be involved in this.

When you have been able to farm out work to Attorneys General, Mr. Smith, does that involve a State enforcement mechanism only, or are there damages requested? Do you ever outsource that to the

Trial Bar in enforcing anything that the FTC does? So, if you could comment on that, I'd appreciate it.

Mr. SMITH. OK. Thank you.

So, I'll go with the resources first.

At this point, we haven't identified any costs that we can't cover, but we do appreciate very much the additional funding that the House Appropriation Committee has recommended for the Commission in FY-2021. We also appreciate the extra resources that we got in FY-2020. And whatever resources we get, we will put to good use.

I will say that we do, though, have two very specific needs. The first is a—legislation to address our authority under Section 13(b) of the FTC Act. So, this is the primary provision that we use to return money to consumers. And, for decades, courts across the country have said that we have authority to obtain equitable monetary relief under Section 13(b).

Very recently, the Court in the Seventh Circuit has questioned that. And so, this is the first court to do that. The great weight of the authority is still on the FTC's side, but this is an issue that has been teed up in front of the Supreme Court for next term. And we expect the Court to resolve that issue by the middle of 2021. But, an adverse ruling from the Supreme Court would mean that the FTC would lose the ability to get any monetary relief under Section 13(b) of the FTC Act, as we have been doing for decades. Because the stakes are so high, we're asking Congress to act now to ensure that the FTC can continue returning money to consumers.

Second issue where we could use some help is reauthorization of the SAFE WEB Act. SAFE WEB Act was last reauthorized in 2012—right? 2012. It will sunset on September 30 of this year. It extends the FTC's UDAP authority—unfair and deceptive practices authority—to conduct that has a reasonably foreseeable effect on U.S. consumers or that involves material conduct in the U.S. This allows us to address cross-border fraud, which is a real problem. Since 2015, we've had 310,000 complaints from U.S. consumers against foreign businesses.

The other thing that SAFE WEB allows us to do is more easily exchange confidential investigative information with our foreign counterparts. We've relied on SAFE WEB to respond to 162 information-sharing requests from 40 enforcement agencies in 17 foreign countries. It's been a critically important tool. And a lot of the COVID-19 fraud that we see is also coming from overseas or Canada.

So, two things that we could really use help with: 13(b) and SAFE WEB.

The—with respect to State AGs, we routinely have task force—we participate in task forces, regular meetings with our State AG counterparts. They will frequently be co-plaintiffs in our cases, particularly charity cases, where they have better authority than we do to return money to consumers. We sometimes refer cases to them. They sometimes refer cases to us. We have—you know, one of our biggest recent cases was our \$170 million settlement with Google and YouTube. That was a case that we did with the New York Attorney General. Critically important—

The CHAIRMAN. Do they farm it out to the Trial Bar——

Mr. SMITH. We have not——

The CHAIRMAN.—the State Trial Bar?

Mr. SMITH.—we haven't farmed anything out to the Trial Bar, and our State partners, as far as I know—we've been dealing with, you know, Assistant Attorneys General; we haven't been dealing with private lawyers who are hired by the Attorney General. In my experience, that's been what we've seen.

But, I haven't, also, been participating in a lot of these task forces. That's generally done by the folks in our regional offices. So, I can't say for sure about outsourcing to the Trial Bar, but I've never heard of it in our cases.

The CHAIRMAN. Mr. Chairman, we're way over time. The—I would note that you and Senator Thune, Senator Blackburn, and I, and Fischer, have a data privacy bill that would deal with this specific issue with COVID-19. And, perhaps on the record, our witnesses might tell us if they've had a chance to look at that, and if they want to go ahead and, on the record, enthusiastically endorse this great piece of legislation.

Thank you, Mr. Chairman.

Senator MORAN. Mr. Chairman, would you like the witnesses to respond to that question now?

The CHAIRMAN. I'll be glad to. I just don't want to intrude on your time. But, if they can respond within your constraints, I'd be—I'd love to hear——

Senator MORAN. Let's do it very quickly.

Derek Schmidt.

Mr. SCHMIDT. Thank you, Mr. Chairman.

Based on the sponsors, I have no doubt that it is excellent legislation, but I have not had a chance to review it.

Senator MORAN. That probably means you're offending half of the members of the U.S. Senate, but——

[Laughter.]

Senator MORAN.—Senator Blumenthal and I continue our efforts in this regard.

Mr. Smith.

Mr. SMITH. So, you know, I can't speak for the Commission, but I—we, institutionally, believe that contract-tracing legislation would be a big help. Consumers really need to be able to trust these contact-tracing apps if they're going to work. And the app developers need to know the rules of the road. So, having legislation—Commission has testified in favor of broad privacy legislation, but, that failing, contact-tracing legislation would be great, too.

Senator MORAN. Mr. Sjouwerman. Is this within your domain?

Mr. SJOUWERMAN. I have not been able to look at this particular bit of legislation, so I can't afford an opinion. Of course, these things are incredibly important. They cover part of the problem. If you take this just a slightly bit more to the 30,000-foot level, you would like to see Federal/national cybersecurity standards, not the patchwork of current different States' cybersecurity standards, which can prevent a multitude of these types of scams in a variety of ways. But, maybe we can come back to that particular issue a little later.

Senator MORAN. Yes, sir, thank you.

Ms. MacCleery.

Ms. MACCLEERY. We'd certainly be pleased to review the bill, but I haven't had a chance to focus on data privacy, I regret to say.

I do have more information on the funding-and-resources question, if that's of interest to the Chair.

Senator MORAN. I'll try to make certain that you—each of you have an opportunity to respond at the end of the hearing to kind of catch up with anything that you would like to add to your testimony.

Let me turn now to Senator Klobuchar, who's been patiently waiting.

**STATEMENT OF HON. AMY KLOBUCHAR,  
U.S. SENATOR FROM MINNESOTA**

Senator KLOBUCHAR. Thank you very much, Mr. Chairman, and thank you, to Senator Blumenthal as well, for holding this really, really important hearing today.

I think we all know that we are in, yes, a public health crisis, but also an economic crisis. And, sadly, when that happens, there are people who prey on people's vulnerabilities. While scammers have used—as you pointed out at the beginning of your remarks, Senator Moran and Blumenthal—they've used the coronavirus to exploit Americans' fears, the impact of the scam on seniors have been particularly disturbing. Reports have come that eight out of ten people in this country who have lost their lives to coronavirus are seniors, and that the seniors, who also lose an estimated \$3 billion annually to financial scams in their normal time, have been targeted for additional scams.

Just last week in my state, we had a scammer that pretended to be the child of an elderly Minnesotan and convinced that person to send \$25,000 to address—an address in Connecticut, not to pick that out, Senator Blumenthal, but, yes, Connecticut. That's why Senator Moran and I introduced the Protecting Seniors from Emergency Scams Act in May to help prevent scammers from taking advantage of seniors during the pandemic. And we've also called on the FTC to protect seniors from some of the contact-tracing scams that you've all discussed, and to educate seniors on how to protect themselves.

So, I think I would start with Ms. MacCleery. Could you talk about how it is critical for seniors and their caregivers to have access to resources from law enforcement, adult protective agencies, to help combat these coronavirus scams? And also, with the rise of online-shopping fraud in which consumer products are ordered online, what is the FTC doing to protect seniors from these type of scams?

Ms. MACCLEERY. Thank you so much, Senator.

I so appreciate the care that you and the Chairman are showing for this very vulnerable population. We know from our work, that seniors, for example, are very heavy users of dietary supplements. Eighty-two percent of people ages 55 to 64, and 88 percent of those 65 and older, take vitamins and supplements, and we've been very concerned that the supplements actually deliver on the benefits that are promised on the label. We sued CVS, several years ago, for producing a supplement or—that was a CVS labelled product

that promised to have macular degeneration ingredients in it that were effective, and, in fact, lacked those ingredients, even though it was sold next to a product that had the appropriate ingredient. So seniors are particularly vulnerable to supplement scams in the way that we've highlighted. They also tend to be vulnerable to the kinds of marketing scams in the supplement marketplace; that is, you know, buy-back guarantees and money-back promises and phishing scams related to those kinds of product marketing. So, that's of real concern to us, and their health makes them more vulnerable to gaps in those supplements or the use of the supplements as substitution for valid medical treatment. It may displace a visit to a doctor that's actually needed.

Senator KLOBUCHAR. Yes. Thank you.

Mr. Smith, I'll direct this one toward you. Is the FTC planning to take additional measures to better protect seniors, assist them with this if they're a victim of a contact-tracing scam? And I know the FTC is coordinating with the DOJ and HHS to warn consumers. Can you highlight the key measures the FTC is taking as part of this coordination?

Mr. SMITH. Sure. Older Americans have been a priority of ours for a long time. You know, interestingly, our research shows that older Americans are not necessarily victimized at a higher rate than younger people. In fact, they're victimized at a somewhat lower rate. But, they suffer more losses when they do suffer a monetary loss. And some of that has to do with scams, like the grandparent scam that Senator Klobuchar outlined, which is really pernicious and can lead to big losses. And so, our efforts are—in addition to our law enforcement efforts, our efforts are focused on educating consumers, particularly to these scams.

And one of our most effective tools has been a campaign called "Pass It On." And what "Pass It On" does—it's a series of articles, presentations, bookmarks, activities, videos, and what it does is, it educates—it's targeted at older Americans, and it says, "Look, you need to give this information to your friend, to your neighbor, to your family member. You need to educate them about this scam." And it allows older people to capitalize on their life experience and their wisdom in educating others. And, of course—and in educating others, they're also educating themselves. So, we've distributed millions of pieces of this information, and we've found that it's effective. But, you're absolutely right, there are always new scams, particularly those involving technology, tech support, contact tracing, which are going—where they're going to find—the scammers will find fertile ground with older consumers.

Senator KLOBUCHAR. OK. Thank you.

Mr. Schmidt, one last question. In your testimony, you note the legislation enacted in Kansas to protect the privacy of consumers' personal data. Do you think that providing strong protections for consumers' personal data is helpful in making these contact-tracing apps more effective? And what more do you think we should be doing federally on the personal data? We're—a number of us have been trying to work on privacy issues—Senator Cantwell, otherwise, as well, when it comes to personal data. And this goes way beyond the pandemic. I think that's only put a magnifying glass on

this issue with the tech companies and the like. But, what do you think would be helpful?

Mr. SMITH. Right. So, the Commission has testified in favor of data security legislation that would include civil penalty authority, APA rulemaking authority, and expanded jurisdiction for the FTC over common carriers and nonprofits. A majority of commissioners have testified for something similar with respect to privacy legislation. And speaking just for myself, I think that privacy legislation would be really helpful now to both tell app developers and others who might be working on contact-tracing issues—let them know what the rules of the road are, what's protected, what they can collect, what the contours of de-identified and aggregated data are, as an example. And it also would build confidence by consumers. Consumers need to be confident in these apps if they're going to use them and if they're going to be effective.

Senator KLOBUCHAR. That's for sure.

Mr. Schmidt, could you also answer that one?

Thanks.

Mr. SCHMIDT. You know, we've obviously followed with interest many of your discussions and debates in Washington on broader privacy issues. And, of course, from a state standpoint, we always have generalized concerns about preemption, the tension between State authorities, on the one hand, and, on the other hand, the benefits of a national standard. Setting that bigger issue aside that I assume would also be a challenge for you at this point if you were trying to do something quickly on this federally, Kansas did—our legislature was in special session in June and did, at that point, enact, at the suggestion of our office, what we call the Contact Tracing Privacy Act at the State level. It's, I think, fairly characterized as stopgap legislation. It sunsets next May. It's designed to fill the immediate need while we have, perhaps, a more thoughtful review of what the law to look like with respect to contact tracing.

It has multiple parts, some of which are not relevant to your question. But, essentially, it requires that—you know, contract—contact tracing was largely unregulated, even though it has deep roots and is a critically important public health tool. At least in Kansas, there weren't many rules of the road. It just sort of was operated the way the public health officials chose to operate it. And, obviously, the scale of the COVID response has brought a lot more people into that business and, therefore, invited discussion about what the rules ought to be.

So, our new statute does things, such as requiring—specifying that participation in contact tracing, whether it's electronic or whether it's the old-fashioned way, with pencil and pen and knocking on a door, is voluntary. We think that's important, because it reduces some of the pushback that some citizens have when the government tells them they “must” provide information, under some sort of penalty. Our statute—again, a stopgap—actually, flat, prohibits the use of cellphone location information, so most of the apps for contact tracing. Our public health department at the State level said they weren't interested in doing that at this point, and we thought it advisable to put the whole thing on hold until there can be a more thoughtful review of what exactly the rules ought to be on that. Again, in the spirit of trying to reassure folks that

it's OK to participate without having to wonder what happens to your information.

And we also, in that statute, ensure that there can be what I've called "bureaucratic mission creep." We ensure that the data lawfully and appropriately collected for contact tracing for COVID, when it's no longer needed for that contact-tracing purpose, must be safely and securely destroyed, because there's obviously going to be tremendous value in a lot of this data, for reasons we may not even have thought about yet, and that may be beneficial. But, again, folks may be really discouraged from participating if they think it's an open door to what their information might eventually be used for.

So, that's been our approach.

Senator KLOBUCHAR. OK. Thank you.

Thank you, Senator Moran.

Senator MORAN. You're welcome, Senator Klobuchar.

Now Senator Fischer.

**STATEMENT OF HON. DEB FISCHER,  
U.S. SENATOR FROM NEBRASKA**

Senator FISCHER. Thank you, Mr. Chairman. I appreciate you holding this hearing today.

American consumers have had to become suspicious of all types of fraud that comes to their e-mails, to the telephones, to their mailboxes, and sometimes to their front doors. On top of this, the coronavirus pandemic has been a convergent of all of these potential scams and—it's increasingly difficult to determine what's real and what isn't.

We saw this recently in my State of Nebraska, when consumers were confused after they received their valid stimulus money from the CARES Act in the form of prepaid debit cards from the U.S. Treasury, and many of them thought it was a scam, so they threw them away. Thankfully, the Treasury has been responsive on resolving these issues.

We've also seen some skepticism from consumers contacted from government agencies for contact-tracing efforts.

Mr. Smith, in light of these, going forward, what can we do to improve trusted channels between the Federal Government and——

Mr. SMITH. Well, what we're doing at the FTC is educating consumers about contact tracing and the like so that they can be—because what—we want consumers to engage with contact tracers. And so, we don't want them simply to be afraid and to shut down when they get that e-mail. And so, our message is, "Don't be afraid to engage with contact tracers, but the first thing is, don't click on any link in that text message," just like General Schmidt said.

Second, the—a contact tracer—a legitimate contact tracer will never ask you for money, for your bank account, for your Social Security number, or for your immigration status.

In addition, on our website, [FTC.gov/coronavirus/scams](https://www.ftc.gov/coronavirus/scams), we have contact information for all the different State Boards of Health and other information about contact tracing to educate consumers about legitimate contact tracing.

But, you're absolutely right that we need to build trust—or consumers need to be able to trust these apps if they're going to work in the way that they're intended to work.

Senator FISCHER. What are you looking at for best practices there? Are you trying to reach out to State government more to be able to work together so that we can build that consumer confidence?

Mr. SMITH. Well, we have—we've issued a great deal of business guidance, including business guidance for contact tracers and for app developers, where we've been counseling app developers to build—to employ privacy and security, by design, at the beginning of the app development process, not simply build it in at the end; that they include privacy protective design features for their apps, such as decentralization of data, so the data lives on individual devices rather than in one centralized database; that they use anonymous data, or, even better, aggregated data, so thinking of heat maps for coronavirus for these contact-tracing apps. They use the data only for the stated purposes. Just like General Schmidt said, if you're collecting it for public health, you use it for that, you use it for nothing else. And you delete the data when you're—when you no longer need it.

So, those best practices would be relevant to a private entity developing a contact-tracing app or to a State Board of Health that's developing a contact-tracing app.

Senator FISCHER. OK, thank you.

And, General Schmidt, I notice that you commented on the enforcement actions that your office recently has taken related to COVID-19 scams. As you've carried out those investigations over the last few months, do you feel that there has been adequate and proactive coordination from the FTC as well as the Justice Department with State AGs on these COVID-related issues and other issues as well?

Mr. SCHMIDT. Yes, I do, Senator. We've had—we have a very good preexisting relationship with our counterparts at the relevant Federal agencies, both in regional offices, to the extent they're in Kansas City at least, or nationally, to the extent they may not have a regional presence in Kansas City. And I think those preexisting relationships have been really helpful in allowing us to simply apply how we normally work together in this context. So, I feel very good about that.

As I suggested in my opening, I think there might be some room to, maybe, in a more institutional way, not—I don't mean legislation, just in a more institutional way, to ensure that relationships that cause cases to flow Federal-to-State or State-to-Federal, for example, between the investigation and prosecution stage, that that may happen even when there are changes in personnel, because so much of it becomes based upon those personal relationships, and, you know, like, you have to reinvent the wheel. But, beyond that, I feel good about it.

Senator FISCHER. OK, thank you.

Thank you, Mr. Chairman.

Senator MORAN. Thank you, Senator Fischer.

We're pleased to have the Ranking Member of the Full Committee here, Senator Cantwell.

**STATEMENT OF HON. MARIA CANTWELL,  
U.S. SENATOR FROM WASHINGTON**

Senator CANTWELL. Thank you, Chairman Moran. And thank you to my colleague, Senator Blumenthal, for being the Vice Chair of the Committee and for all your hard work on these issues. It's great to join you.

And I think what I'll try to do is just talk about some very, very broad issues, if I could. I think my colleagues have covered a lot of territory. And, first of all, let me just thank you for mentioning—and my colleague Senator Klobuchar—the data security issue. Really feel that data security is, and should be, included. So, thank you for endorsing that concept, that data security really does need attention, along with privacy legislation overall. So, thank you for that.

On this issue of the—you know, the usual FTC approach, which is a first-time warning, do the witnesses agree that the FTC needs a first-time civil penalty authority when it comes to some of these COVID, you know, deceptive information and statements, given the severity of the problem?

I don't know, Ms. MacCleery, I don't know what you have to say, or whether Mr. Smith wants to comment on that.

Ms. MACCLEERY. So, I think that the warning-letter tool has limitations. There are a number of unscrupulous actors in the marketplace that may disregard warning letters, and it's enormously inefficient for the FDA or the FTC to have to track and go after bad actors multiple times. We have seen a pattern, even in supplements tainted with drugs like amphetamines. The agency will issue a warning letter, and then the company will come back with a slightly tweaked product and keep selling into the same marketplace. So, I think, for supplements in particular, you have a small number of bad actors, and warning-letter authority is just insufficient to get their attention.

Senator CANTWELL. Well, we—definitely agree. We were very involved in drafting a new law as it related to, you know, the same on our opioid crisis. We didn't put enough oomph behind the penalties there. So, I think we should look at this. I mean, you know, a civil penalty, given something that's about protecting the lives of individuals in the middle of a pandemic, when people are reaching, you know, for solutions, seems a reasonable approach.

Mr. Smith, did you want to add anything to that? I have a different question for you. So.

Mr. SMITH. OK. I would just say, I think your question was about, like the opiate law, where, under Section 5, we bring an enforcement action, and we're entitled to equitable monetary relief, an injunction, things like that, but no penalties. Right? And if we get an administrative order for the second go-round, we can get civil penalties. And so, I think that's what your question was focused on, not so much the warning letters. And I would say—

Senator CANTWELL. I'm saying, I think the warning letters, in the middle of a pandemic, on things that people might think are lifesaving, when actually they're, you know, causing—

Mr. SMITH. Right.

Senator CANTWELL.—fatalities—could cause fatalities, seems like a warning letter may not be strong enough, given the complexity

of this environment we're in. And giving the FTC a stronger tool——

Mr. SMITH. Right. Well, so we have a stronger tool. We can go to court, with all—with respect to every one of the companies that we've sent a warning letter to, we can go to Federal court or in front of our administrative law judge, and we can get an injunction. We have chosen the warning-letter route because what we have found with—particularly with respect to the fake cures, what we have found is that the warning letters are astonishingly effective. In 48 hours, we can get bad claims taken down. And where we can't, we follow up with law enforcement, either in a Federal court or in front of our administrative law judges.

Senator CANTWELL. Well, what about flexibility?

Mr. SMITH. I'm sorry——

Senator CANTWELL. I mean——

Mr. SMITH. And then I think what you're——

Senator CANTWELL. I mean, just like what Ms.——

Mr. SMITH.—advocating is another path, where we get civil—like with the opiate law, where we get civil penalties on our first bite at the apple. And with respect to that, that's a better question for the Commission. I would be getting pretty far out over my skis if I were to offer an opinion——

Senator CANTWELL. OK. What——

Mr. SMITH.—on whether we——

Senator CANTWELL.—about——

Mr. SMITH.—should have civil penalties.

Senator CANTWELL. What about our definition of price gouging? And I don't know if—I mean, this unfairness authority. I mean, that's what we, in Washington, prevent unfair and deceptive practices pretty similar, I think, to where you guys are, but it is quite broad. So, do we need to do more on defining the price-gouging standard?

Mr. SMITH. I think we—yes. It would be helpful to have a price-gouging statute. If Congress wanted us to address price gouging specifically, it would be really helpful to have a statute that gave us specific authority and laid out specific guidelines for when—for, basically, what high—what—how high is too high? So, 35 states which have the same FTC Act authority that we do—you know, they have the Unfair and Deceptive Acts or Practices authority—they have, nonetheless, seen fit to enact a price-gouging statute, because the unfairness authority doesn't fit neatly. So, that would be—if you want us to address price gouging, a statute——

Senator CANTWELL. But——

Mr. SMITH.—would be a big help.

Senator CANTWELL. Well, we have one for you, so we will—we'll get that.

Mr. SMITH. Right.

Senator CANTWELL. So——

Mr. SMITH. Right.

Senator CANTWELL. I mean, we've been involved in establishing a standard for you also on manipulation, and we thought that was quite helpful, and very helpful to the CFTC, and very helpful for the FERC. So, we think clarity, here, is our friend, and we think——

Mr. SMITH. Right.

Senator CANTWELL.—or, just like with the opioid law, I think if people can get around it, they will. And so, the stronger deterrent that we can have on the books, in the penalties, the better, in my opinion.

One last question I was going to ask about. Let's see. What else do we need to do on some of these—you know, some of the larger organizations that have taken advantage of states on their paychecks and the programs for unemployment?

Mr. SMITH. So, are you talking about large businesses that have obtained, for example, paycheck protection program loans?

Senator CANTWELL. I'm talking more about the abuse of the system, of people signing up and getting—you know, rings of people who have signed up to get—in the State of Washington——

Mr. SMITH. Right.

Senator CANTWELL.—we've had——

Mr. SMITH. Right.

Senator CANTWELL.—employment checks given to rings of——

Mr. SMITH. Right.

Senator CANTWELL. Yes.

Mr. SMITH. So, I would say—so, General Schmidt, from Kansas, may have some thoughts on that. From the FTC's perspective, when we see the—I think from—we send it to the IRS or to their—TIGTA—to their Inspector General for—because that's real—that's real criminal theft, right?

Senator CANTWELL. Yes.

Mr. SMITH. From the government.

Senator CANTWELL. Yes.

Mr. SMITH. And so, it's not so much an FTC problem. But, General Schmidt may have additional thoughts. I don't know.

Senator CANTWELL. Well, I just want to know what we're doing to share that, you know, data, in general. Obviously, identify theft and these issues are something that the FTC—so, don't know many——

Mr. SMITH. Right.

Senator CANTWELL.—other states have addressed this, or faced it, but—I don't know——

Mr. SMITH. So, we do——

Senator CANTWELL.—if General Schmidt has something—I mean, if the—yes—General Schmidt wants to offer something.

Mr. SCHMIDT. Senator, the only thing I might add, as I mentioned but didn't dwell on earlier with respect particularly to unemployment benefits, which may or may not be precisely what you're asking about but it's a similar genre, we have gotten a lot of complaints from folks alleging—broaden those benefits payments, identity theft, creating false identities to claim a payment. The way we've been handling those—because, under Kansas law, I don't have original criminal jurisdiction for that type of crime—so, the way we've been handling those is to refer them to our State Department of Labor, which handles unemployment program, and they, in turn, then work with their Federal counterparts whenever, in their judgment, it's appropriate to do so. So, a little bit outside, under Kansas law, of our authority.

Senator CANTWELL. OK. Thank you.

Thank you, Mr. Chairman.  
 Senator MORAN. Senator Cantwell, thank you very much.  
 Senator Capito.

**STATEMENT OF HON. SHELLEY MOORE CAPITO,  
 U.S. SENATOR FROM WEST VIRGINIA**

Senator CAPITO. Thank you, Mr. Chairman, and thank the Ranking Member, for having this hearing. Very interesting, and it's interesting—I'm just going to kind of start on the—where Senator Cantwell left off, and that is the fraud on the unemployment compensation.

We just had—I'm from West Virginia—we just had an instance, where our unemployment commissioner, basically, said that somebody from the same IP address had applied for 50,000 different ways to get a benefit with, you know, different names, or tweaking different names. And I'm wondering—Attorney General Schmidt, you mentioned that this is an issue that's come up in Kansas, but I'm wondering, is it the magnitude of which we're seeing? And also, what additional resources would you need to combat something of this nature, when the program was created this rapidly but also to the great benefit of so many people?

Mr. SCHMIDT. Senator, from the vantage point of the Kansas Attorney General's office, we haven't seen that scope, but I'm quick to say we might not, because, as I was just describing to Senator Cantwell, we aren't necessarily the face of the public response.

You know, the only thing I might add—it's something we have talked and thought about a big here, because we've seen the reports in other states, that the problems have been widespread, and I don't have a reason to think that Kansas is materially different. I just have not seen the data.

Senator CAPITO. Right.

Mr. SCHMIDT. But, you know, there are other programs, where there is a Federal/State partnership, as there is now with the unemployment payments coming from the Federal Government to assist and extend the benefits. Medicaid program comes to mind. And, in some of those programs, Congress has seen fit to create certain requirements for fraud policing by the state in order to participate in the program. For example, the Medicaid Fraud Control Units that I mentioned earlier.

So, I am not prepared to advocate that in the unemployment insurance context, but I—it does seem to me a logical area to look, whether that model for programs that have shared funding would also make sense in the unemployment context for shared fraud enforcement.

Senator CAPITO. Yes. I mean, I think it—a lot of our systems are very overwhelmed, as you know. And to try to determine where the fraud lies and how to detect it, I think, is—

I'm going to stick with you, Mr. Attorney General, because I want to ask something that comes up in this committee all the time that has to be related to scams, and certainly the education of either our elderly or others. And I appreciate Senator Klobuchar bringing up the scamming of the elderly. That's an issue I'm very concerned about, in all aspects. But, you know, we have a lack of broadband in our rural areas. And what do you find is the best way

to really transmit, to people who may not have broadband connectivity, the possibility of false advertising or false claims or, you know, cures that are going to cure it all or prevent you from ever getting COVID? What—how do you address that issue in Kansas?

Mr. SCHMIDT. So, we are the lead consumer protection agency for the State, at the State level, in Kansas. And, because of that, in ordinary times, we have a very robust consumer education and prevention program. We do it online, as you suggest. We also do a lot of in-person presentations around the state, whether it's civic clubs, nursing homes, senior centers. We—our people spend a large proportion of their time actually talking with Kansans, because our philosophy is, "If we can help you avoid losing your money in the first place, better for you, it's better for us, so we can focus our enforcement on the back end, on a smaller universe."

Senator CAPITO. Right.

Mr. SCHMIDT. So, that's how we normally do it.

Now, as your question, I think, implies, right now, where we're all less mobile, we're doing things, like we're doing today, in communicating remotely. Obviously, that disables one of our principal tools for reaching Kansans, which is, "Go where they are, in person, and talk with them." And so, we've struggled with that. We are doing more online. We recognize the limits, as you suggest, that there are areas that that's simply not going to be effective because our consumers aren't able to access that programming. But, nonetheless, we think there is a significant number of Kansans who we don't normally reach online, we could reach online—technologically they're able—and so, we're doing that now, because it's better than not doing anything. So, we've pushed that.

But, I have struggled very much with how we reach those pockets of individuals in the state that we can't reach digitally because they don't have suitable Internet access, and we can't reach them physically right now because of the—

Senator CAPITO. Right.

Mr. SCHMIDT.—of the COVID-related restrictions. And I don't have a good answer right now.

Senator CAPITO. Yes. I think that's a real problem, because a lot of those are our more vulnerable populations, and I think it brings a difficult question.

I don't know if I have any more time. I've got one more question to Mr. Smith.

We've seen a big increase in scams, obviously. And they're heading toward the vulnerable population, which we've said. But, what limitations to the FTC—this is to my FTC—let's see—yes, Mr. Smith—what limitations does the FTC have? And I've created an Act, with Senator Gardner, called the CEASE Act, which would increase penalties for false advertising and deceptive acts. Wondering if that would be a helpful tool, if you're aware of it, and what tools—additional tools you might need at the FTC to be able to break up these large advertising scams that we see.

Mr. SMITH. Right. So, I am familiar with the CEASE Act. And we are—I think we may have provided some technical assistance—

Senator CAPITO. Yes. Thank you.

Mr. SMITH.—for your offices. And we are happy to continue working with your office on that law.

And with respect to specific tools that we could use, I mentioned, earlier, reauthorizing the SAFE WEB Act. I think Senators Moran and Blumenthal have introduced—have cosponsored a bill that would reauthorize the SAFE WEB Act. That's critically important for our foreign law enforcement. And some of these COVID scams are coming from outside of the country.

Senator CAPITO. Right.

Mr. SMITH. The second thing is to clarify our authority under Section 13(b) of the FTC Act. So, for decades and decades, we've had authority to obtain equitable monetary relief under Section 13(b). And, just recently, there have been—there has been one important court, the Seventh Circuit Court of Appeals, which has called into question that authority. That issue is now in front of the Supreme Court. It will probably be resolved sometime next year about this time. But, in the meantime, it would be great if Congress could act to clarify our authority that we can get redress, restitution, disgorgement as Congress has thought we've been able to get for the last, what, now probably 40 years.

Senator CAPITO. Right.

Thank you very much.

Senator MORAN. Senator Capito, thank you.

A vote has been called. And I have been very lenient in time. I'll try to be less so now. I'm sorry.

Senator Udall, it's now your turn.

**STATEMENT OF HON. TOM UDALL,  
U.S. SENATOR FROM NEW MEXICO**

Senator UDALL. Thank you, Chairman Moran and Ranking Member Blumenthal, for calling this hearing on the important issue of protecting our constituents from COVID-19 scams.

There is unprecedented demand for products to protect against the transmission of coronavirus. And the scramble to keep our families, workers, and customers safe has led to a surge in scams and fraud against consumers. The FTC has received over 136,000 reports of scams related to COVID-19, including 477 from New Mexico. And people have reported losing nearly \$90 million on these and other COVID-related frauds.

But, it's not just individual consumers that are at risk, here. There are increasing reports of companies misrepresenting themselves in contracts with local, State, and Federal agencies to procure PPE.

In May, a \$3 million Indian Health Service contract was given to a former White House official to provide 1 million KN95 respirator masks for use in the Indian Health Service facility serving the Navajo Nation that did not meet—these masks did not meet the Food and Drug Administration's standards for use in healthcare settings by healthcare providers.

I want to address the issue of some substandard masks. Thousands of masks procured by IHS were determined to be substandard and not for medical use for IHS hospitals serving the Navajo Nation in New Mexico and Arizona. I brought this up in another hearing directly with the IHS Director and told him that this

was absolutely unacceptable. Thankfully, the masks were never used, but HHS and FDA ought to be pretty savvy consumers when it comes to workplace safety in the medical field.

I'll have a written question for our in-writing witness from the FDA.

But, Ms. MacCleery, what can this administration do to better protect workers, both in the private sector and government? And do you support an OSHA emergency standard?

Ms. MACCLEERY. Absolutely. We are on record as supporting OSHA's development of an emergency temporary standard for workers at risk of contracting COVID. We've particularly been worried about meatpacking workers, where we've seen a large number of exposures and deaths, both among inspectors and workers. And it may be something about the working conditions and the close proximity there that lead these to be hotspots. Workers really need these protections in order to maintain our food supply and keep going to work. And we need a healthy workforce. So, we are backing the measures that have come out of the Congress in several packages for an emergency temporary standard for workers.

In addition, we think there should be a concerted effort to, of course, develop mask standards for workers in the healthcare setting. We know there's some of that going on underway. But, some sort of concerted attention by the FDA to set standards is needed. Masks in the healthcare setting have been to protect the patient from infection by the healthcare worker, not necessarily to protect the worker. And so, there needs to be a new and urgent effort to ensure that workers in the settings where they're dealing with patients are also protected.

Senator UDALL. Ms. MacCleery, are online platforms doing enough to put a stop to questionable and fraudulent goods before they are sold?

Ms. MACCLEERY. There certainly has been a concerted effort by Amazon and a few of the other platforms to work with Federal authorities and get rid of explicitly marketed COVID cures and treatments. However, behind that there is lots more work to do. In general, we need to have a plan for when platforms are selling supplements to the public, and the false claims that they're making, and for actively patrolling them, not just during a pandemic. And in addition, not all platforms are making enough of an effort. We have looked across a number of the platforms, and not all of them are free of products that are explicitly promising to treat or prevent coronavirus, which is a problem.

Senator UDALL. Thank you.

Mr. Chairman, knowing that a vote is on and we're pressed for time, I'll submit the rest of my questions. I really believe there is a role for Attorneys General to play here, and I hope that our witnesses will answer that question on the record.

But, I will yield back at this time.

Thank you very much.

Senator MORAN. Ever so cooperative. Senator Udall, thank you very much.

Senator Baldwin.

**STATEMENT OF HON. TAMMY BALDWIN,  
U.S. SENATOR FROM WISCONSIN**

Senator BALDWIN. Can you hear me?

Senator MORAN. Yes, ma'am.

Senator BALDWIN. Can you see me? That's the other question.

Senator MORAN. Now we can.

Senator BALDWIN. Yes. OK. Thank you.

So, thank you, Mr. Chairman.

This March, I introduced a bipartisan bill to incentivize states to provide compensation to elderly victims of financial fraud, abuse, and exploitation. I called it Edith's Bill after learning the story of Edith Shorougian and her family, who wrote a letter to me, asking that I work on legislation to help seniors get money back when it's stolen from them, especially when it's money earned over a lifetime of hard work.

General Schmidt, do you believe that elder financial fraud and abuse is underreported? And are you aware of any national programs or efforts that would incentivize states to provide compensation or restitution to these victims if they're unable to recover restitution from the offenders themselves?

Mr. SCHMIDT. Senator, I absolutely believe that elder fraud and abuse, including financial abuse, are underreported. All of the data I've ever reviewed—and it has been substantial—suggests that there's a quarrel about how much—to what order of magnitude the underreporting is, but not about the principle.

In terms of your question about compensation, I'm not aware if—just I'm not aware of it—of any program that provides compensation to elder victims of crime. There is, of course, the Crime Victims Compensation Program, generally, that I'm sure all of our states participate in. Generally speaking, that compensation, as I recall, is limited to certain categories of costs that generally are associated with violent crime, as opposed to financial losses.

We make a priority, in Kansas, in our enforcement actions, to put restitution first and the State's recovery always second. And, of course, that usually is more important at the collection stage than it is at the liability-imposition stage. But, in principle—I don't know any particular proposals, but, in principle, I think it would be a very good conversation to talk about whether there's some type of compensation program that would assist somebody's who's lost a life savings as the result of fraud and scams.

Senator BALDWIN. So, thank you for that. Edith and her family were scammed out of more than \$80,000 by their longtime financial advisor. And, of course, they fear that they'll never get that money back that was stolen from them. But, Edith's family was able to uncover the fraud because Edith asked for help, and her son-in-law recognized that there was a problem when he was attempting to reconcile and balance her checkbook.

General Schmidt, in April, you led a letter to Senate leadership in which you and other Attorneys General noted that emergencies and disaster situations invite abuse and exploitation of vulnerable and isolated populations. So, I want to know if you are concerned that seniors who are isolated from family members, loved ones, caregivers during the pandemic, and the support networks that they usually rely on, are being targeted by scammers. And how

does this separation from typical caregivers make seniors more vulnerable and susceptible to such scams?

Mr. SCHMIDT. Senator, this is one of the things that keeps me up at night right now. We have focused tremendously, in both the Kansas Attorney General's office and then a couple of years ago, when I was President of our National Association of State Attorneys General. We focused on elder abuse issues, including financial abuse, on a national basis from a State standpoint. So, it's a long-standing priority for us.

I am very worried that seniors who may be physically isolated, ordinarily, and have their contact come to them, or—in terms of home healthcare or other home support—or who go to contact, but in very discrete manners—they go to a doctor's office visit, they perhaps go to their coffee klatch for lunch on every Thursday, and back, but they're now separated from those de facto early warning systems that can spot something out of the ordinary and perhaps sound the alarm, as happened with your constituents. I am very worried about that.

And I might just say—I don't mean to sound like a broken record; I highlighted it in my testimony and mentioned it in my opening statement—but, I really do believe that one step that Congress could take swiftly, I believe without controversy, would be to include in some vehicle this year, perhaps the next COVID bill, whatever is appropriate, the text of Senate bill 2379, which is the latest incarnation of legislation that we've been working on now for several years. From a state standpoint, we began the advocacy—it was actually, at that time, Attorney General Jepsen, from Connecticut, and myself, bipartisan—asking for this change in statute so that we can use our existing, already-funded, already-trained, already-skilled resources in our Medicaid Fraud Control Units outside the exit doors of the nursing homes and long-term care facilities, and reach exactly the type of isolated individuals in the Medicaid program that you're talking about.

So, thank you.

Senator BALDWIN. Thank you.

And, Mr. Chair, I think my time has run out, so I yield back.

Senator MORAN. Thank you very much.

Senator Sinema has joined us, as well.

Senator Sinema.

#### **STATEMENT OF HON. KYRSTEN SINEMA, U.S. SENATOR FROM ARIZONA**

Senator SINEMA. Well, thank you, Mr. Chairman.

And thank you, to all of our witnesses today.

Scammers are using this pandemic as an opportunity to defraud Americans, including our seniors. Arizonans have reported thousands of COVID-related scams to the FTC, with \$1.5 million in losses for Arizona families, so far. And those are just the scams that are reported to the FTC. We know the actual damage is far greater.

Scams aren't just a financial concern. COVID scams also endanger the health of the public, who can be defrauded into believing that certain products can prevent or cure COVID, when, of course, there's no scientific basis to support these claims.

Scammers have also distributed counterfeit personal protective equipment, which can endanger lives of our medical professionals and first responders. I'll continue to work with partners on the Federal, State, and local levels to ensure we have adequate resources to prevent scams before they happen, ensure that we're returning funds to Arizona fraud victims, and punishing the scammers who are stealing from our families.

Before I move to questions, I want to thank Senator Capito for mentioning our bill to extend FTC authority to stop false advertising during this pandemic. Our bill increases civil and criminal penalties on scammers, and we hope to find some bipartisan support for this legislation.

My first question is for Attorney General Schmidt. Due to the coronavirus pandemic, scammers are using fear and confusion to steal money and personal information. Recently, I teamed up with our Attorney General, Arizona Attorney General Mark Brnovich, to warn Arizonans about some common coronavirus scams. This includes trying to sell fake coronavirus vaccines or unproven treatments to scared families and individuals. Scammers are also calling seniors and threatening to cutoff stimulus payments or food assistance if they don't share personal information. You know, this criminal behavior not only hurts the direct victims, but it also hurts legitimate charitable initiatives who are trying to help vulnerable communities respond to the virus.

My question for you, Attorney General, is, How can policymakers help our constituents distinguish between scams and legitimate offers of assistance? And are there additional resources that states need in order to more effectively fight these new pandemic-related scams?

Mr. SCHMIDT. So, Senator, it is such a difficult question, because mixed messaging is the bane of effective messaging. And we normally all are on the page of, "Don't answer the phone. Don't respond to the inquiry. Just hang up on the bad guys if you don't know them." Now we're in a position where we're saying, "Well, that's all true, but, you know, we sure like you to respond, for example, to contact tracers when they engage with you," and that creates a really difficult message to convey to vulnerable populations.

I don't know that I have a great answer. I can tell you what my messaging is when I talk with Kansans about the types of things you're saying. I usually say it boils down, for me, to two simple points:

How do you separate the legit from the illegitimate? Number one, if you didn't initiate—you as the Kansan, you as the Arizonan, you as the consumer—if you didn't initiate the contact, the communication, then just assume it's not legit. Now, that gets me in trouble with some legitimate both businesses and public-sector folks, but, from a consumer-protection standpoint, it is a simple, straightforward message. If you want a widget and you think you need a widget, sit at your breakfast table, figure that out, initiate the contact with the seller of widgets, and now you know at least you're in contact with a legitimate operator. So, that's point one.

And point number two, you know, the old-fashioned advice is still good. Do business—whether it's online, remotely, or in person, do

business with people you already know and trust. So, shop local or shop reputable retailers in the retail space.

Again, it's not perfect, but those two principles are usually what I tell folks.

Senator SINEMA. Thank you, Attorney General. I appreciate that.

My next question is for Mr. Smith. As part of the fight against the coronavirus, many organizations have experienced severe shortages of PPE, cleaning and disinfectant supplies, and other necessary items that would help them reopen safely and smartly. As the virus continues to surge in places like Arizona, our local businesses, schools, nursing homes, and healthcare facilities are continuing to struggle to buy supplies from their usual and trusted vendors. What advice do you have for businesses and organizations that want to buy PPE or other coronavirus-related supplies in order to avoid fraudulent or counterfeit materials?

Mr. SMITH. Well, our efforts with respect to PPE have largely been focused on what I'll call shop-at-home scams, or fulfillment scams, where a company is offering to sell PPE, and you order the PPE; it says, you know, "next-day delivery," and it's not delivered next-day; in fact, it's delivered "never." So, we're not—so, the folks that we're protecting are generally consumers and not businesses. And we've brought at least one enforcement action in that area, and we have several more in the pipeline. I would say that, you know, what we are enforcing there is our mail-and telephone-order rule, which requires that, if you're not going to deliver on time, that you provide a notice or the opportunity for a full refund.

With respect to those larger institutional purchases of PPE that you're talking about, we also have been working with the Department of Justice, which has been extraordinarily active under the Defense Production Act, both—and a lot of our PPE fulfillment issues have followed on their price gouging under the DPA. So, there are unscrupulous sellers out there, selling counterfeit products, price gouging, taking advantage of institutions' needs for these products in this time of emergency. And so, a lot of that, I think, is being addressed by the criminal authorities, and, in particular, the Department of Justice and the Department of Justice DPA Price Gouging Task Force.

Senator SINEMA. Thank you.

Mr. Chairman, my time's expired, but I want to thank you for holding this important hearing. I appreciate it.

Senator MORAN. Senator Sinema, thank you.

Senator Blackburn has joined us, as well.

Senator Blackburn.

**STATEMENT OF HON. MARSHA BLACKBURN,  
U.S. SENATOR FROM TENNESSEE**

Senator BLACKBURN. Thank you so much, Mr. Chairman.

And I want to go to the issue of data privacy. And, General Schmidt, you mentioned this in your statement. And let's look at the issue of protecting that private information, and then, if that falls into the hands of scammers, what are you doing to make certain that people are not being scammed based on their information for this contact tracing? Because what we've learned—when you look at the virtual space, whoever has that data and claims posses-

sion of that data feel that they know—that they own the “virtual you.” They have access to this and then begin to use that entree to follow you and to share your information with outsiders and third parties.

So, General Schmidt, let’s talk with you—or start with you, and then just, if each of you will add. I want to hear about what is being done to protect privacy, to protect that data, to protect the follow-on information via contact tracing.

Mr. SCHMIDT. Senator, I appreciate the question. You know, I don’t mean to sound glib, either to you or anyone who’s listening, but often in this space, I think of the old expression that “the road to hell is paved with good intentions.” And I worry, in the contact-tracing space, because we have grown so rapidly into that data collection, that perhaps we have not put in place the ordinary safeguards we would otherwise put in place with any entity, government or business, that’s collecting large amounts of personal data. And we’ve done it for good purposes, to try to properly contain the spread of the virus. But, I’ve been sort of the contrary voice on that, and I’ve done it deliberately, because I think we need to have a more balanced conversation.

As I suggested earlier, and I won’t repeat myself, but we did, in Kansas, our legislature, in June, enacted what I’ve characterized as a stopgap contact-tracing privacy act data-privacy measure. It’s designed to put in place guardrails, rules of the road, duties of privacy, limitations on distribution, and the like, for all of that data that’s collected, both the digital stuff that we’re talking about, in terms of app development here, but also data that’s collected the old-fashioned way. Still, once it’s collected and in the data base, it does have value to some folks. And so, we have tried to put in those limitations to make sure that Kansans’ data is protected and they can feel free to participate openly in legitimate tracing efforts.

Senator BLACKBURN. Let me ask you this. First of all, what I’ve heard you say is, we need to have a Federal preemption and one Federal standard for the retention—collection of, and retention of, this data. Is that correct?

Mr. SCHMIDT. Senator, yes, with a—an important caveat. And that is this. And this is my State role coming out. I do understand the importance of a Federal standard. It makes sense. Data crosses State lines. I understand that. But, I would suggest that we don’t want complete Federal preemption of State enforcement. And—

Senator BLACKBURN. Correct.

Mr. SCHMIDT.—we also don’t want—

Senator BLACKBURN. [Inaudible]—

Mr. SCHMIDT. Yes, but we also don’t want to compel State—for example, State AGs—to go to Federal court, follow Federal rules to enforce a Federal law, because, with all respect, as I’ve said to my colleagues many times, if I wanted to do that, I’d try to go be a U.S. Attorney. I’m a State actor. So, it’s always seemed to me what makes the most sense is to set a Federal standard with respect to data privacy, but to allow states to independently enforce that standard under State law, in State court, with State procedures and State rules, as long as we’re holding folks to the same standard.

Senator BLACKBURN. Yes. Let me ask you this before we move on. And my time is about to run out. Should, then, we see that—should it be that consumers—the online consumer has the ability to choose to opt-in to share their information, or choose to opt-out if they do not want that entity that is collecting and holding that information to share that with third parties? Is that a—something that should be granted to them, or a protection afforded to them?

Mr. SCHMIDT. Well, it does seem so to me, Senator. And obviously, as you know probably better than I, that that's at the core of a very broad and robust policy debate, both here and with our friends in Europe. But—

Senator BLACKBURN. Correct.

Mr. SCHMIDT [continuing]. It—I am on the general side of the debate that suggests my personal data is my personal data, and I ought to be able to control with whom it is shared and then re-shared and reused.

Senator BLACKBURN. All right.

I'll tell you what, Mr. Chairman, with that I'm going to yield back, in the interest of time.

Thank you.

Senator MORAN. Thank you for yielding back.

I've got to go vote. I have one question I want to ask, and then I'm going to turn the hearing over to Senator Blumenthal for a question or two he may have. He's going to then close the hearing.

We are to be exiting this room by 5:45, so our panel of witnesses should breathe a sigh of relief that it can't last much longer.

I want to ask Mr. Sjouwerman. The—with the noteworthy cybersecurity news related to Twitter last week serving as a pretty significant example of social engineering, these types of attacks continue to evolve while posing increasing harm to Americans. Your testimony indicated that these types of threats are responsible for, quote, "upwards to 93 percent of data breaches." Do you have any recommendations for this subcommittee on how Congress can draw increased consumer attention to these risks, or even prevent them from occurring in the first place?

Mr. SJOUWERMAN. Yes. There is—ideally, there should be Federal/national cybersecurity standards. There are several standards. For instance, the National Institute of Standards and Technology—they are abbreviated as NIST—they have several standards in place. The problem is that if you want to really combat social engineering attacks, you're going to have to go far and wide in—you're going to have to get the private sector, to some degree, involved and motivated to live up to data security and privacy standards.

If you had asked me, What is the best framework to use in this particular case?—I'd point you to the Department of Defense, the Cybersecurity Maturity Model Certification. This is abbreviated as CMMC. They have a very good model, where you have five levels of ramp-up, in the sense of making sure that you comply more over time and can buildup your resilience against scams like this. And the—basically, the ultimate or very effective solutions for all the scams that you see is awareness. Train the elderly in increased awareness. And the AARP is actually doing a good job of that. It's an awareness issue. Educate, but also protect. And the standards of protecting just the home PC, but also corporate networks, should

ideally be a Federal standard so that everyone can comply, because, at the moment, it's a patchwork. And, as we can see, it isn't working.

Senator MORAN. Mr. Sjouwerman, thank you very much.

Thank you, to all the panelists, for your presentation today.

General Schmidt, thank you for joining us from home. Derek, I've known you at least since you were a young Kassebaum Senate staffer. And thank you for your public service, now, for a long period of time on behalf of our fellow Kansans. I appreciate your presence with us today, but appreciate your presence in Kansas and what you do for all of us.

I now—

Mr. SCHMIDT. Thank you, Senator.

Senator MORAN.—recognize Senator Blumenthal.

Senator BLUMENTHAL [presiding]. I want to join in thanking you, as a former fellow Attorney General, and just say, the next time we have a hearing with you as a witness, maybe we can do it out in Kansas instead of here. And I want to—

Mr. SCHMIDT. Always welcome, sir.

Senator BLUMENTHAL. And I want to ask you specifically, because—Mr. Smith has said he would welcome a price-gouging law at the Federal level, and I completely agree, because right now there really is no Federal price-gouging law, and that is a great obstacle to effective Federal enforcement. And I encountered this issue when I was State Attorney General, urging the then-Attorneys General of the United States to take action, and the FTC, and they said to me, "Well, we have no Federal law." And in Kansas, you have a price-gouging law that says that a price increase is presumed unjustified if it exceeds by 25 percent the pre-crisis level. Tell me how you feel about that law, whether you think it has helped or harmed your office's ability to bring enforcement action, and whether you would recommend it to us in the U.S. Senate, in the Congress?

Mr. SCHMIDT. Senator, it—I think it has been useful for Kansas. As Mr. Smith has suggested a couple of times, sure, we could—prior to enactment of that law, we could try to use our general Kansas version of the UDAP authority—we actually don't have an "unfair" standard, but we have a "deceptive or unconscionable" standard—to deal with price gouging. But, it is really clunky to do that, and it's much better if there's something that looks more like a bright-line standard. That way, everybody knows what the rules are. And our experience has been, by having that on the books, with that 25-percent presumption, it has allowed us to get voluntary compliance, almost universally, at least from legitimate actors. Now, you know, the crooks and scammers are crooks and scammers. That's a different category. But—of course, when you're talking about price regulation, you're talking about, at least to some extent, dealing with very legitimate enterprises, and the bright-line rule in law is very helpful in bringing them into compliance without the need for formal enforcement. At least it has been for us.

Senator BLUMENTHAL. Clarity is always good for enforcement.

Let me ask you. And this is a little bit of an unfair question, because Senator Moran is not here. If we were to adopt a Federal

statute, I personally would be against making it preemptive of all State laws, broadly preemptive. I don't know how you feel about that issue of preemption when it comes to either price gouging or other Federal statutes.

Mr. SCHMIDT. Yes. Senator, you know, philosophically, as I suggested early on—I'm a states' guy, and so, not surprisingly, I'm not a fan of Federal preemption, generally, as a philosophical matter. Now, having said that, I recognize there are times it makes perfect sense. As I just suggested to Senator Blackburn, you know, data privacy, I understand why you can't have, as a practical matter, 50-plus, with territories, different sets of standards for folks to manage data privacy. So, the one thing I say on that—and I—you know, I'm quick to say—this is always true, but it's particularly true in this area—I—I speak only for myself—I have colleagues among the State and Territory Attorneys General community who have very different views on this—but, speaking for myself, when Congress has made the determination, appropriately, by subject matter, for a Federal standard, as a—in some area; let's say, data privacy or maybe it's on price gouging, whatever it is—as a general matter, if that's going to be what Congress does, and it's going to preempt states from having a different standard, my own preference would be, don't go further than that in the preemption. Don't preempt me from having a State law that codifies, in State law, the same standard—so, it's the same performance that's required of the regulated entity—that I can then enforce independently, under State rules and State court, with our State procedures, because that's what my team is accustomed to doing. And perhaps, in some larger States, where they have very large, let's say, consumer protection shops, they have folks who are accustomed, every day, to going down and litigating in Federal court and enforcing Federal law. Maybe it's a HIPAA statute, or whatever it may be. But, that's not true for us, and I think it's not true for a lot of smaller states.

And so, as I'm making enforcement decisions, just to be, you know, blunter than I should, but just to make the point—I'll overstate it—I mean, I got enough to do enforcing the laws of the State of Kansas that I was hired by my voters to enforce. Enforcing Federal law is not a great privilege that I aspire to, it's something else to do. It's not very high on the pecking order. So, I would much rather, if Congress is going to set a standard, set it, but then let me work with my legislature, perhaps in addition to letting me go to Federal court—I have no objection to that, but don't make it my exclusive option—let me work with my legislature to find a way that we can bring State law alongside and enforce that standard our way.

Senator BLUMENTHAL. Thank you. I appreciate your perspective, which I think is very valuable.

On the—on this topic of privacy, I want to ask you, Mr. Smith. Contact-tracing apps are not regulated under HIPAA or any other privacy laws. I've introduced bicameral legislation to regulate these apps. The proposal is called the Public Health Emergency Privacy Act. But, isn't there more that the FTC could do? I know you've issued general guidance, but nothing recent, and nothing specific,

so far as I'm aware, such as advisory notices to the tech company—

Mr. SMITH. Right.

Senator BLUMENTHAL.—to the technology companies, that I am aware of, about consumer privacy of contact-tracing apps. If this system of contact tracing is going to have any chance of working, privacy has to be assured to consumers. That's the FTC's job. And I'm concerned that the FTC has been silent.

Mr. SMITH. So, the privacy of contact-tracing apps we would address now, in the absence of any special Federal legislation, using our unfairness and deception authority. And I can't comment on any specific companies or any specific investigations, whether we might have them open or not. But, this is an area where we have been heavily focused. And part of that is because consumers—you're right, consumers have to trust these contact-tracing apps if they're going to work. We need a lot of uptake in order for contact-tracing apps to work.

App developers also need to know the rules of the road. So, we have recently—I'd say within the last month—issued business guidance to app developers, where we have five or six specific points that they should take into account when developing apps. Now, some of these aren't going to be anything new to you, like privacy by design, for example. But, there is one that's kind of interesting, which is, use privacy protective design features, such as decentralized protocols. So, one of the things that I think is really interesting about these contact-tracing apps that we've been running into recently is that they don't actually collect everybody's location in one big centralized data base, and everybody's health information in one big centralized data base. It lives here. And it is—and I have my Bluetooth turned on, and you have your Bluetooth turned on, and it has a—these devices all have a single Bluetooth identifier. And if I test positive for coronavirus, then that gets uploaded to the data base, and you dial into the data base, and you see, "Is anyone in any of these Bluetooth IDs that I've been in close proximity with—is it in the data base, or not?" So, by using those kinds of decentralized protocols, we solve a lot of privacy issues up front. Other guidance—which, again, no surprise—you know, don't use identifiable data, use aggregated data, to the extent you're able. Some of these apps will do things like display heat maps for where there's particular risk of exposure. So, they—you don't need to know—you don't need to have even unique personal data, much less personally identifiable data. Aggregated data will do just fine.

So we have, within the last month or so, I think, issued business guidance for app developers. But, you're right that this is an area where we need to be vigilant, and we are heavily focused on it, because this is kind of the—this is the privacy issue for 2020.

Senator BLUMENTHAL. It is one of the key privacy issues, and it has such sweeping ramifications, as you know as well or better than I. And I'm just thinking that more clarity and specificity, with more information made available to the public—I'm aware of those protocols, the decentralization, use of Bluetooth. Amazon and Google are working on systems. There is a coalition of groups that's hoping, I think, to have it ready by the end of this summer. But, I think an explanation to the American public about how this data

is safe, what those rules of the road will be, and how they will be impervious, or at least highly protected, against intrusion or interference, I think it would be very valuable——

Mr. SMITH. That's an excellent——

Senator BLUMENTHAL.—to make these——

Mr. SMITH.—point.

Senator BLUMENTHAL.—systems work.

Mr. SMITH. Our consumer ed, so far, has focused more on how to spot a contact-tracing scam, right? You know, which is the, “Don't click on a link. If they ask you for money, it's not legitimate,” that kind of stuff. But, you're right, in order to build trust, we might need to—have to, you know, actually explain, “Look, this is what a contact-tracing app does, and how it works.”

Senator BLUMENTHAL. Because, as you know—as you well know, contact-tracing doesn't work unless you reach a threshold level of——

Mr. SMITH. Right.

Senator BLUMENTHAL.—participation. And right now, we ain't nowhere near——

Mr. SMITH. Right.

Senator BLUMENTHAL.—anywhere in this whole country. And very few places in the world, if any, have reached that threshold level. So, you know, we talk so broadly and frequently about, “We need testing, we need contact tracing, we need a vaccine, we need therapeutics,” and, in some ways, the contact tracing may be the most difficult of all——

Mr. SMITH. Right.

Senator BLUMENTHAL.—to achieve, because we don't have that trust and credibility.

Mr. SMITH. Right. And I don't know—I mean, so—I'm not, sort of, up to date, as of today, but I do not believe that there are very many State Boards of Health that have contact-tracing apps. And I think that—I mean, Kansas has passed its contact-tracing law, but I have heard only of one or two states that have developed these apps. And then, of course, the apps are going to have to be able to work together, right? Virginia will have to speak with Oklahoma, and the different APIs, whether it be Google or Apple, will have to work together. So, it's a significant challenge.

Senator BLUMENTHAL. Right. Well, we could talk about a lot more. I have one more area of questioning that I want to cover.

You mentioned that the warning letters are, I think you said, “effective,” maybe even “very effective.” Maybe, in some cases. But, I talked about 255 warning letters. A lot of those scammers have come back, maybe not with exactly the same language, but they—they're back, and, in some part, due to the lack of vigilance on the part of the tech platforms that I mentioned earlier, and Ms. MacCleery very articulately described, need to be held more accountable.

But, I just want to say, about warning letters, speaking as a prosecutor, you know, I used to try to get actual court judgments, not even consent order. Because you get a consent order, you have to go back to court to enforce it. With a warning letter, you have nothing to enforce. It's no deterrent. If you're—if you leave here, and you drive above the speed limit, 85 miles an hour in a 60-mile-

an-hour zone, and you get a warning letter, the deterrent effect, especially if you know that, the next time, you'll get another warning letter, has very little impact.

So, I wonder whether a more aggressive use of—whether it's administrative or actual judicial process for judgments, for fines, for even criminal referral, wouldn't be appropriate.

Mr. SMITH. Right. So—well, there's a lot there. And I agree with you, 100 percent, that a warning letter, by definition, is a warning letter; there is nothing to enforce. But, in the last—let's say we've been at this for over three and a half months, middle of March—maybe 4 months—and in that time, we have succeeded in getting almost all of those 255 companies to take down the claims. And for those that haven't—there are some, and there are some that have taken the claims down, only to replace it with something that's equally misleading—we are pursuing law enforcement action, both in Federal court and in front of our administrative law judges. You've seen the fruits of some of that, and it's outlined in our testimony. There's a lot more of that in the pipeline, though. But, those cases take time. And particularly when you're talking about fake cures, the way that we will typically prove that up is with expert testimony, to say, you know, "Here's what scientific, you know, educated people in the profession would say is adequate substantiation, and you ain't got it." That takes time. It also takes money. But, you know, I think we have the resources, I think we have the manpower to do it. We are doing it. But, it's not something that can be easily done overnight.

And so, you know, these warning letters have been very fast and very effective, I think. And, when not, then we back it up with law enforcement. But, you're absolutely right that a warning letter, on its face, is not worth much.

Now, General Schmidt, though, said that, with respect to price gouging, that a lot of the challenge is just telling companies that are legitimate, more or less, that, "Hey, look, you can't do this. You can't say this." And when you do that—you know, if we can fix the problem by—through that kind of communication, then we need to—then we need to be—we need to be doing that.

But, I appreciate your concern, absolutely.

Senator BLUMENTHAL. Yes. I think there are all kinds of different potential violations. Some are close to the line, some are in the gray area. You know, when you recommend the equivalent of somebody swallowing hand-sanitizer or something like that—

Mr. SMITH. Right.

Senator BLUMENTHAL.—or bleach, or whatever—and you're making money from it—

Mr. SMITH. Right.

Senator BLUMENTHAL.—I think that something more than a warning letter may be appropriate. But—

Mr. SMITH. Well, they're also—we also have been with the FDA, as you know.

Senator BLUMENTHAL. Yes.

Mr. SMITH. And FDA has been—as they outlined in their testimony, they've been bringing some actions criminally. We have been making criminal referrals. So, we work with a wide variety of partners. And sometimes, in some of our most pernicious cases, when

we get there, we realize that the crimes are involved, too. And so, we will defer to them, unless they want us to come along with them, which has happened in a couple of cases. Because we can sometimes get relief more quickly than they can. You know, they can do their search warrant and, at the same time, we can get our, you know, asset freeze and receiver appointed.

Senator BLUMENTHAL. Thank you.

At the risk of being tossed out, which has not yet happened to me as a Senator, tossed out of the room, I'm going to close the hearing. But, I am certainly interested in following up on many of these issues.

I want to thank each of our witnesses—Mr. Smith, Attorney General Schmidt, Mr. Sjouwerman, and Laura MacCleery—all of you, for your excellent testimony, and, more important, for your excellent work. You are trying to make these laws work. We make the laws, but you try to make them work. And I really appreciate your being here today. I'm sure the Chairman joins me in that sentiment. And I hope we have an opportunity to talk soon again.

This hearing record will remain open for two weeks. During this time, Senators are asked to submit any questions for the record. Upon receipt, the witnesses are requested to submit their written answers to the Committee as soon as possible.

I, again, thank the witness—witnesses for being here.

And this hearing is adjourned.

Thank you.

[Whereupon, at 4:51 p.m., the hearing was adjourned.]



## A P P E N D I X

### RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JERRY MORAN TO DEREK SCHMIDT

*Question 1.* Your office continues to lead robust enforcement efforts to identify and prosecute individuals engaged in COVID-19 related fraud, and I thank you for those efforts. Our state attorneys general are on the “front lines” when it comes to protecting consumers during this pandemic, and we are committed to assisting them as appropriate during this difficult time. Keeping in mind that many consumers often report fraud and scams directly to state and local authorities, how can Congress assist with some of the obstacles that agencies like the Kansas Attorney General office face every day when dealing with out of state criminal operations?

Answer. We work closely with the Federal officials in Kansas, and especially the Kansas City regional offices of several Federal agencies. We appreciate the open lines of communication we have with those agencies to refer cases when the bad actor is outside our jurisdiction—particularly those operating from overseas. I would continue to encourage Congress to invest resources in these regional office as well as any efforts that encourage collaboration between the state and Federal agencies with jurisdiction.

*Question 2.* What does coordination between your office and your Federal law enforcement partners, like the FTC, currently look like?

Answer. Our office routinely refers cases to Federal law enforcement partners, including the FTC. We have participated in several nationwide “sweeps,” when state and Federal officials nationwide have filed enforcement actions in a coordinated time period, which helps to raise awareness that both state and Federal government officials are focused on enforcing laws that protect consumers. Our office has participated in sweeps focused on elder fraud and fraudulent activity in the student loan market, to name two examples.

*Question 3.* Both the state of Kansas and the FTC have pursued enforcement actions against fraudsters posing to be government entities like the Small Business Administration (SBA) aiming to dupe consumers into sharing personally identifiable information or money. Are there specific protocols that you each have in place that distinguish the treatment of these types of frauds differently than others?

Answer. Impersonation scams constantly rank among the top types of scam reports our office receives. This includes everything from the classic “grandparent scam” to tech support scams. But, those impersonators who claim to be calling from a government agency are among the most egregious. We have even received reports of scam artists calling and claiming to be from the attorney general’s office. Our protocols for investigating these scams do not differ significantly based on the type of impersonation the scam caller is purporting to be. We do regularly alert consumers to these types of impersonations when we hear of them—including recently advising consumers of SBA impersonation scams that have been reported, claiming to help small businesses receive assistance from the various COVID-relief programs.

*Question 4.* Outside of general interstate jurisdictional concerns, would you explain all the factors that your office takes into consideration in determining what cases to refer to your Federal law enforcement partners?

Answer. The primary factor is the subject matter of the case we are working, and the Federal regulations/agencies with jurisdiction to that subject. We take into consideration the size/impact of the case, sometimes measured in victims, sometimes in dollars. We have long-term working relationships with several agencies, and those serve us well in assessing our course of action with our Federal partners.

*Question 5.* While many businesses have taken well-intentioned steps to develop technological solutions to tracking, containing and ending the COVID-19 pandemic, Congress must address potentially harmful practices that could stem from these innovations if not held accountable. On May 7, I joined Chairman Wicker and other colleagues in introducing the COVID-19 Consumer Data Protection Act of 2020, which would require companies collecting individuals’ sensitive personal data for

contact tracing or other COVID-19-related purposes to obtain affirmative express consent.

a. Would you please describe the recent efforts of your office to protect consumers from harms associated with the collection and processing of their personal data in contact tracing processes?

Answer. In early June, the Kansas Legislature passed the COVID-19 Contact Tracing Privacy Act as part of its COVID-19 response package passed during the 2020 Special Session. I recommended the Contact Tracing Privacy Act be included in that legislative package and assisted in drafting its contents. That legislation, which contains provisions that I believe to be common-sense measures to reassure Kansans that they can participate in contact tracing without worrying about the security of the information they provide to contact tracers, sunsets in May 2021 and is designed as a stopgap measure to put basic privacy and civil liberties protections in place while our state legislature conducts a more thorough review of public policy options. The legislation includes the following provisions:

- Consistent with CDC guidance, participation in contact tracing must be voluntary. No person may be required to participate, nor forbidden from participating.
- Contact tracing may not collect information through cellphone tracking and may not use any information collected through cellphone tracking.
- Information collected through contact tracing must be used only for contact tracing, kept confidential and not disclosed. The information must be safely and securely destroyed when no longer needed for contact tracing.
- Only specified information may be collected by contact tracers. The list of information that may be collected must be established by the Secretary of Health and Environment through the open and transparent process of adopting formal rules and regulations.
- The government may not require any third party to collect contact data. Information voluntarily collected by third parties may only be obtained by the government with the consent of both the third party and the person the information relates to, or with a judicially supervised warrant.
- People working as contact tracers must receive training and must affirm that they are familiar with the privacy and civil liberties protections in the legislation.

Additional information on this bill is included in my Op-Ed published on National Review Online, which was attached to my written testimony.

---

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DAN SULLIVAN TO  
DEREK SCHMIDT

*Question 1.* We have seen various scams relating to this pandemic, including scams related to Federal relief efforts such as the PPP and economic impact payments (EIPs), as well as health-related scams that sell fake PPE and tout false cures and treatments for the virus. What do you believe is the most prevalent scam right now relating to the pandemic? And what should Americans and Alaskans most be on the lookout for to avoid it?

Answer. Please find attached a copy of my recent Consumer Corner column, which is distributed to media across Kansas. In that column, I outlined the five most-common COVID-19 scams that have been reported to our office, which includes the scams mentioned in your question.

*Question 2.* As everyone knows, we are currently negotiating another relief package that will potentially contain resources that could attract scammers. Are there steps that Congress, the FTC, or the states could take to proactively prevent future scams as the pandemic continues?

Answer. When the CARES Act was being negotiated earlier this year, we anticipated scam artists would begin to use the “stimulus payments” as the basis for new scams. We began to warn consumers of this even before the CARES Act was passed by Congress, and advised consumers to only trust information coming from the official government websites, such as the IRS and SBA. Referring consumers to those agencies’ websites was key to stopping the spread of false information and assuring Kansans of how to know if information, checks or the prepaid debit cards they received from the government were legitimate. I hope that if another relief package is passed, those agencies will continue to proactively provide information to keep consumers informed and know how to spot false information and scams.

In addition, as discussed in my written testimony, I encourage Congress to enact as part of any further COVID-19 relief legislation S. 2379, which would immediately remove a Federal impediment to use of existing state Medicaid Fraud Control Units to detect, investigate and prosecute the abuse of Medicaid beneficiaries in non-institutional settings. These existing assets could immediately be available to protect Medicaid beneficiaries from financial abuse by scammers if this legislation were swiftly enacted.

*Question 3.* How have the States and the FTC, along with the various Federal agencies, been working together to combat these scams?

Answer. As mentioned in my written testimony and the above answer to Senator Moran's Question 1, we have been working closely with the FTC and our regional Federal agencies. We appreciate the information sharing that is taking place on how to protect consumers and the ability to refer complaints and cases to the Federal agencies when appropriate.

---

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JERRY MORAN TO  
ANDREW SMITH

*Question 1.* The FTC's authorities provided by the U.S. SAFEWEB Act are critical to maintaining cross-border cooperation on consumer protection investigations and fraud actions with our foreign law enforcement partners. These authorities expire in a couple months, and Senator Blumenthal and I introduced a necessary reauthorization that awaits Senate floor consideration. How would the expiration of these authorities impact the FTC's ongoing enforcement efforts related to COVID-19 scams and other unfair and deceptive acts?

Answer. SAFE WEB is an indispensable part of the FTC's enforcement arsenal. It provides the Commission with critical law enforcement tools to combat fraudulent telemarketing, robocalls, privacy violations, misleading health claims, spam, spyware, malware, and other cross-border misconduct that harms American consumers. Without SAFE WEB, the FTC might not prevail in enforcement actions against foreign wrongdoers. SAFE WEB contains an express provision stating that the FTC's authority over unfair and deceptive practices extends to foreign conduct that has a "reasonably foreseeable" effect on U.S. consumers, or that involves "material conduct" in the United States. Without SAFE WEB's "clear statement of Congressional intent," FTC enforcement against foreign wrongdoers would be in jeopardy.

SAFE WEB also supports cooperation with foreign counterparts against unlawful cross-border activity, efforts that are even more critical in the current COVID-19 environment. We have identified many businesses in foreign jurisdictions targeting consumers in the United States with advertisements for products they falsely claim will treat, prevent, and cure coronavirus and illegal robocalls coming from abroad touting a wide variety of coronavirus-related financial scams. We have already used our SAFE WEB authority to exchange confidential information about coronavirus-related scams with foreign enforcers.

*Question 2.* Your testimony indicated that the FTC's coordinated efforts with the FDA in sending warning letters to marketers for false treatment claims have been successful in many cases, especially when coupled with enforcement actions as appropriate. Would you describe the general process and roles of the two agencies in identifying and enforcing against these types of threats? How do these efforts differ when addressing COVID-19 prevention or treatment claims made by major multi-level marketing companies?

Answer. Continuing our strong tradition of close cooperation, the FTC has coordinated closely with the Food and Drug Administration to identify and target sellers of unproven COVID-19 remedies. When addressing COVID-19 prevention or treatment claims made by major multilevel marketing companies, the FTC's approach remains the same as with other types of sellers. While we obtain information about potential frauds from many sources, including searches on the Internet and social media platforms, FTC staff also perform a daily review of COVID-19-related complaints submitted by consumers to our Consumer Sentinel database, and these complaints are a critical source of investigative leads. After issuing the warning letters, we monitor each company that received a warning letter. If the claims at issue persist, we contact the company to ensure compliance, and we proceed with law enforcement action as warranted.

*Question 3.* With the noteworthy cybersecurity news related to Twitter last week serving as a significant example of social engineering, these types of attacks continue to evolve while posing increasing harm to Americans. Does the FTC success-

fully pursue enforcement actions against these socially engineered cyber-attacks? Do they coordinate with Department of Justice and state attorneys general in such efforts?

Answer. Although we defer to criminal enforcement authorities in bringing cases against the cyber attackers themselves, the FTC has engaged in numerous activities to ensure that businesses protect their customers' information from socially-engineered cyberattacks. The FTC's business guidance emphasizes that, under various statutes enforced by the FTC, businesses must design a security program that addresses foreseeable risks, including training staff on basic security measures, such as phishing attacks and other forms of social engineering. The FTC has also brought law enforcement actions against companies that have failed to implement reasonable security training. And, the FTC has engaged in research and training on novel forms of social engineering attacks. For instance, in January 2020, the FTC held a workshop on voice cloning technologies that can enable attackers to create a near-perfect clone of someone's speech based on a five second recording of a person's voice. The workshop included a panel devoted to methods of authenticating, detecting, and mitigating the risks of these technologies.

We also cooperate regularly with state and Federal law enforcement agencies in data security matters. For example, in the Equifax case, where we alleged a lack of reasonable employee training, we cooperated with 50 state attorneys general. As to cooperation with criminal authorities, while we have not made such cooperation in particular cases public, we regularly communicate with our criminal counterparts as we bring enforcement actions, through our Criminal Liaison Unit within the FTC.

*Question 4.* Would you please describe the FTC's efforts to coordinate with the Federal Communication Commission and industry, particularly the USTelecom Industry Traceback Group, in identifying, mitigating, and enforcing against fraudulent robocalls related to COVID-19?

Answer. In an effort to quickly and efficiently stop illegal robocalls that used a coronavirus-related message, the FTC sent 15 (as of 08/18/20) warning letters to VoIP service providers and providers of caller ID numbers potentially involved in these robocalls. Six of those warning letters were sent jointly with the FCC. In its investigative work to identify appropriate recipients for the warning letters, the FTC used information provided by the USTelecom Industry Traceback Group ("ITG"), a collaborative effort of companies across the wireline, wireless, VoIP, and cable industries that actively trace and identify the source of illegal robocalls.

The FTC warning letters to VoIP service providers and other companies warn them that "assisting and facilitating" illegal telemarketing or robocalls related to the COVID-19 pandemic is against the law. The joint FTC/FCC warning letters include a warning that the FCC will authorize U.S. providers to block all calls from recipients of the warning letter.

FTC enforcement attorneys continue to join in regular coronavirus telemarketing enforcement coordination calls with their counterparts at DOJ, FCC, and the offices of state attorneys general. The enforcers also have a regular call with the ITG on fighting robocalls.

*Question 5.* Both the state of Kansas and the FTC have pursued enforcement actions against fraudsters posing to be government entities like the Small Business Administration (SBA) aiming to dupe consumers into sharing personally identifiable information or money. Are there specific protocols that you each have in place that distinguish the treatment of these types of frauds differently than others?

Answer. Government imposter scams are consistently one of the most common issues reported to the FTC, and in times of crisis or distress like the current pandemic, we often see a rise in imposter scams seeking to take advantage of consumers. Frequently working with state and Federal partners, we can quickly pivot to address these scams through enforcement efforts and consumer and business education.

Recently, the FTC has focused on companies posing as the Small Business Administration to businesses seeking CARES Act relief. Businesses that apply for such relief through these companies, as opposed to through legitimate SBA approved lenders, might lose out on the ability to obtain relief. Specific steps we take to uncover these schemes include searching our consumer complaint database, calling victims, coordinating with the SBA, examining targets' websites, and uncovering the individuals involved.

When we uncover concerning practices, we move quickly to stop the conduct, by filing a complaint and seeking preliminary relief in court, or sending warning letters to the companies to curb the conduct. We have taken these types of approaches, including conducting investigations and filing complaints or sending warning letters,

in other areas as well, particularly where companies have sought to capitalize on consumers' financial and health concerns as a result of the pandemic. In general, these are the types of protocols we follow when combatting fraud in any area; however, given the current financial and health crisis, we have devoted additional resources to combatting pandemic-related frauds, including government imposter scams.

*Question 6.* Your testimony described the robust awareness campaign on COVID-19 scams that the FTC has developed in response to the pandemic ranging from staff participation in presentations to rapid response consumer alerts issued by the agency. In response to the COVID-19 pandemic specifically, has there been increased attention dedicated to a particular type of scam based on the frequency of cases that may not have been as prevalent previously?

Answer. While the agency responds to reports of scams with consumer and business education, staff are able to draw on their experience to try to get ahead of scams with clear warnings to the public. For example, the first COVID-19-related blog post from the FTC came on February 20, 2020, ahead of many scams, and a March 18, 2020 warning about the scams that would accompany Economic Impact Payments garnered more than 1.5 million views. The FTC has drafted more than 100 consumer and business blog posts in response to the pandemic, covering a variety of topics, including health and treatment claims, charity fraud, government imposters, contact tracing, privacy, and scams targeting small business. The FTC has held or participated in dozens of webinars, tele-town halls, and conference calls covering these topics with a wide range of groups, including the AARP, FEMA, SBA, FDIC, CFPB, DoD, the BBB, and members of Congress.

There have been some notable surges in scams reported. For example, the agency received a sharp uptick of reports from consumers about online shopping scams—especially complaints about merchandise that is ordered and never received. According to an FTC Data Spotlight report, “[p]eople reported unreceived orders of facemasks in April and May far more often than any other item, and undelivered sanitizer, toilet paper, thermometers, and gloves were also reported.”<sup>1</sup>

The Commission used databases within the agency to track this problem. Based on that proactive monitoring, the FTC recently brought four Federal court cases against sellers of PPE, each of whom we alleged took advantage of consumers' need for quick delivery at the outset of the pandemic by advertising quick turnaround times because they had products in stock. We alleged that, in fact, that they did not have PPE in stock, could not deliver for months, and refused to provide the refunds required by law.<sup>2</sup>

*Question 7.* I remain motivated to provide American consumers with clear and measurable data privacy and security protections in Federal statute, and it is clear that the Federal Trade Commission is the ideal regulating agency for such framework. Contact tracing practices require the collection and processing of sensitive personal data. Based on the FTC's past privacy enforcement efforts under their existing Section 5 authority, would you please describe the importance of any enforcement actions accounting for the sensitivity of the personal data or the potential harm associated with information in question?

Answer. The Commission has long sought to protect sensitive information. Some examples follow:

- *Financial information:* The compromise of financial information such as Social Security numbers, account numbers, and usernames and passwords on financial accounts can lead to a host of injuries, including fraudulent charges, delayed benefits, expended time, opportunity costs, fraud, and identity theft. We have sought to protect this information through recent cases such as the Equifax

<sup>1</sup>FTC Data Spotlight, *Pandemic purchases lead to record reports of unreceived goods* (July 1, 2020), <https://www.ftc.gov/news-events/blogs/data-spotlight/2020/07/pandemic-purchases-lead-record-reports-unreceived-goods>. See also <https://www.consumer.ftc.gov/blog/2020/07/scams-online-sales-when-orders-dont-arrive>

<sup>2</sup>See FTC Press Release, *FTC Acts Against Online Sellers That Falsely Promised Fast Delivery of Facemasks and Other Personal Protective Equipment* (Aug. 5, 2020), <https://www.ftc.gov/news-events/press-releases/2020/08/ftc-acts-against-online-sellers-falsely-promised-fast-delivery>; FTC Press Release, *FTC Takes Action against Marketer That Falsely Promised Consumers Next Day Shipping of Facemasks and Other Personal Protective Equipment* (July 8, 2020), <https://www.ftc.gov/news-events/press-releases/2020/07/ftc-takes-action-against-marketer-that-falsely-promised-next-day-shipping>.

case,<sup>3</sup> as well as cases against a mortgage broker,<sup>4</sup> service providers for auto dealers,<sup>5</sup> and multilevel marketers.<sup>6</sup>

- *Health information:* Unauthorized disclosure of health information can lead to harms ranging from physical harm (e.g., use of stolen health insurance number to get treatment, where the criminal's health records get mixed up with the victim's) to reputational harm that can result from disclosure of stigmatizing health conditions. Indeed, one of the Commission's first health privacy cases involved the unauthorized public disclosure of individuals' Prozac use.<sup>7</sup>
- *Children's information:* Concerns over children's physical safety, as well as concerns over limiting the collection of information about children without parental consent, helped to drive Congress's enactment of COPPA in 1998.<sup>8</sup> The FTC has vigorously enforced COPPA in dozens of cases, most recently against Musical.ly (now TikTok),<sup>9</sup> YouTube,<sup>10</sup> and the developer of the popular KleptoCats app.<sup>11</sup>
- *Geolocation information:* The revelation of consumers' precise geolocation data—particularly in real-time—can lead to physical harms such as harassment or stalking. The FTC has considered this data to be sensitive and has brought enforcement actions against companies that collected or shared this data without consumers' knowledge or consent. For example, the FTC recently alleged that BLU Products violated the FTC Act by transmitting sensitive personal information about consumers—including real-time cell tower location data—to another company's servers in China, without consumers' knowledge or consent.<sup>12</sup>
- *Contents of consumer communications:* The Commission has considered the content of certain private activities to be sensitive. Congress has as well, and, for example, unauthorized disclosure of private video viewing habits led to the enactment of the Video Privacy Protection Act in 1988.<sup>13</sup> In the same vein, in 2017, the Commission unanimously approved a settlement with VIZIO, Inc., a manufacturer of Internet-connected TVs, alleging that the collection and use of sensitive television viewing data from unwitting consumers was an unfair practice.<sup>14</sup>

<sup>3</sup>FTC Press Release, *Equifax to Pay \$575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach* (July 22, 2019), <https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related>.

<sup>4</sup>See FTC Press Release, *Mortgage Broker That Posted Personal Information about Consumers in Response to Negative Yelp Reviews Settles FTC Allegations* (Jan. 7, 2020), <https://www.ftc.gov/news-events/press-releases/2020/01/mortgage-broker-posted-personal-information-about-consumers>.

<sup>5</sup>See FTC Press Release, *FTC Gives Final Approval to Settlement with Auto Dealer Software Company That Allegedly Failed to Protect Consumers' Data* (Sept. 6, 2019), <https://www.ftc.gov/news-events/press-releases/2019/09/ftc-gives-final-approval-settlement-auto-dealer-software-company>.

<sup>6</sup>See FTC Press Release, *FTC Finalizes Settlement with Utah Company and its former CEO over Allegations they Failed to Safeguard Consumer Data* (Jan. 6, 2020), <https://www.ftc.gov/news-events/press-releases/2020/01/ftc-finalizes-settlement-utah-company-its-former-ceo-over>.

<sup>7</sup>See FTC Press Release, *Eli Lilly Settles FTC Charges Concerning Security Breach* (Jan. 18, 2002), <https://www.ftc.gov/news-events/press-releases/2002/01/eli-lilly-settles-ftc-charges-concerning-security-breach>.

<sup>8</sup>See COPPA Legislative History, 105th Congress, 2nd Session, Vol. 144 (Oct. 21, 1998), <https://www.congress.gov/congressional-record/1998/10/21/senate-section/article/S12741-4>.

<sup>9</sup>See FTC Press Release, *Video Social Networking App Musical.ly Agrees to Settle FTC Allegations That it Violated Children's Privacy Law* (Feb. 27, 2019), <https://www.ftc.gov/news-events/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc>.

<sup>10</sup>See FTC Press Release, *Google and YouTube Will Pay Record \$170 Million for Alleged Violations of Children's Privacy Law* (Sept. 4, 2019), <https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations>.

<sup>11</sup>See FTC Press Release, *Developer of Apps Popular with Children Agrees to Settle FTC Allegations It Illegally Collected Kids' Data without Parental Consent* (June 4, 2020), <https://www.ftc.gov/news-events/press-releases/2020/06/developer-apps-popular-children-agrees-settle-ftc-allegations-it>.

<sup>12</sup>BLU Products, Inc., No. C-4657 (Sept. 10, 2018), <https://www.ftc.gov/enforcement/cases-proceedings/172-3025/blu-products-samuel-ohav-zion-matter>; see also FTC Press Release, *FTC Gives Final Approval to Settlement with Phone Maker BLU* (Sept. 10, 2018), <https://www.ftc.gov/news-events/press-releases/2018/09/ftc-gives-final-approval-settlement-phone-maker-blu>.

<sup>13</sup>The Video Privacy Protection Act of 1988, codified at 18 U.S.C. § 2710 (2002).

<sup>14</sup>See Complaint for Permanent Injunction and Other Equitable and Monetary Relief (Feb. 6, 2017), [https://www.ftc.gov/system/files/documents/cases/170206\\_vizio\\_2017.02.06\\_complaint.pdf](https://www.ftc.gov/system/files/documents/cases/170206_vizio_2017.02.06_complaint.pdf); see also FTC Press Release, *VIZIO to Pay \$2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions without Users' Consent* (Feb. 6, 2017), <https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it>.

*Question 8.* Has the agency looked into existing contact tracing technology proposals?

Answer. Yes, the agency has been following this issue closely. Key privacy issues relating to contact tracing or exposure notification technologies include whether health information is collected by companies providing the technology, app developers, or public health authorities, and what other information, such as location data or identifiers that can be linked back to the user, are collected in addition to information about the user's health status. Among other things, agency staff have engaged with various companies to learn more about how the systems work technically, limitations on use of any information collected, and division of responsibility for securing data collected.

We have also issued guidance for companies that plan to engage in partnerships with government entities for pandemic-related purposes. The guidance notes that companies should consider privacy and security as they are developing their initiatives, rather than after launch; use privacy-protective technologies; consider using anonymous, aggregate data; and use data only for limited health-related purposes and delete the data when the crisis is over.<sup>15</sup>

*Question 9.* I think it is essential to the protection of U.S. consumers that they be able to recover money stolen from them by scam artists, and the FTC is our main agency assuring such recovery. However, lately its ability to get money back to victims has been under judicial attack. Mr. Smith, should Congress consider providing additional statutory clarity to the FTC's 13(b) authority in seeking equitable monetary relief on behalf of consumers?

Answer. Yes. Section 13(b) of the FTC Act is one of the FTC's principal tools for protecting consumers. Since the 1980s, courts have applied longstanding Supreme Court precedent to hold that Section 13(b) allows all types of equitable relief, including refunds to consumers. Using this authority, the Commission has secured billions of dollars in relief in every manner of case, including telemarketing fraud, anti-competitive pharmaceutical practices, data security and privacy, scams that target seniors and veterans, and deceptive business practices. Unfortunately, however, our ability to keep getting such results for consumers has been threatened or curtailed by recent judicial decisions. Accordingly, as indicated in my testimony and the testimony of the Commission on August 5, the FTC is seeking legislation to clarify the agency's statutory authority to obtain complete monetary relief under Section 13(b) of the FTC Act.

---

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARSHA BLACKBURN TO  
ANDREW SMITH

*Question 1.* How is the FTC working alongside your partners at DOJ to prosecute bad actors who are duping vulnerable Americans into appalling scams?

Answer. The FTC works closely with DOJ on several fronts to protect American consumers. Notably, the FTC works with main Justice and U.S. Attorneys' Offices through our Criminal Liaison Unit (CLU) to ensure the worst fraudsters are prosecuted and punished. In the first three quarters of this Fiscal Year, FTC staff actively worked on one hundred thirty-one (131) new formal requests for cooperation from our criminal law enforcement partners. Prosecutors relied on FTC information and support to charge thirty-two (32) new defendants and obtained sixteen (16) new pleas or convictions. Six (6) defendants received sentences totaling one hundred ninety-eight (198) months.

Also, the FTC and the FBI are collaborating bring the Internet Crime Complaint Center's consumer fraud data into the FTC's Consumer Sentinel Network, which is the Nation's largest repository of consumer fraud complaints. This information sharing will help the FTC, DOJ, and many other agencies across the country to access investigative leads in a single database, Sentinel.

Further, at the outset of the pandemic, FTC participated in weekly (and now as needed) calls with DOJ and numerous other Federal partners to identify and tackle COVID-19-related scams.

*Question 2.* I understand that the FTC and FCC have been working hand in hand to combat coronavirus-related fraudulent behavior. Can you tell me about the warning letters the FTC, in conjunction with the FCC, sent to service providers and other companies, warning them that "assisting and facilitating" in illegal telemarketing or robocalls related to the Coronavirus pandemic is against the law?

---

<sup>15</sup> FTC Business Blog, *Privacy during coronavirus* (June 19, 2020), <https://www.ftc.gov/news-events/blogs/business-blog/2020/06/privacy-during-coronavirus>.

Answer. In an effort to quickly and efficiently stop illegal robocalls that used a coronavirus-related message, the FTC sent 15 (as of 08/18/20) warning letters to VoIP service providers and providers of caller ID numbers potentially involved in these robocalls. Six of those warning letters were sent jointly with the FCC.

The FTC warning letters to VoIP service providers and other companies warn them that “assisting and facilitating” illegal telemarketing or robocalls related to the COVID-19 pandemic is against the law. The joint FTC/FCC warning letters include a warning that the FCC will authorize U.S. providers to block all calls from recipients of the warning letter.

FTC enforcement attorneys continue to join in regular coronavirus telemarketing enforcement coordination calls with their counterparts at DOJ, FCC, and the offices of state attorneys general. The enforcers also have a regular call with the USTelecom Industry Traceback Group on fighting robocalls.

---

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DAN SULLIVAN TO  
ANDREW SMITH

*Question 1.* We have seen various scams relating to this pandemic, including scams related to Federal relief efforts such as the PPP and economic impact payments (EIPs), as well as health-related scams that sell fake PPE and tout false cures and treatments for the virus. What do you believe is the most prevalent scam right now relating to the pandemic? And what should Americans and Alaskans most be on the lookout for to avoid it?

Answer. While we don’t have survey data to establish prevalence of pandemic-related scams, of consumer complaints to the FTC’s Consumer Sentinel Network that mention terms related to the pandemic (such as COVID, stimulus, N95 facemasks), the largest category involves Online Shopping. As of August 5, 2020, Sentinel had received 23,755 such reports from consumers.<sup>16</sup> Within that category, most complaints are about goods that were ordered and never delivered.

People who shop online should check out any unknown websites before ordering goods, and they can do this by typing the website name into a search engine along with the words like “scam” or “complaint.” They should confirm the seller’s physical address and phone number, and watch out for unfamiliar sites selling products that are in short supply. Finally, they should always pay with a credit card or debit card, and dispute charges for any goods that do not arrive.<sup>17</sup>

The agency has published multiple blog posts for consumers and businesses on PPE, as well as Federal relief efforts, including one I recently authored about unlawful practices targeting small businesses.<sup>18</sup> In addition, FTC staff have participated in dozens of webinars to educate small business owners about PPP-related scams. Because the FTC is regularly posting blogs that cover the most recent COVID-related scams, among others, Alaskans can subscribe to the FTC’s Consumer Alerts (<https://www.ftc.gov/consumeralerts>) and Business Alerts (<https://www.ftc.gov/businessalerts>) to stay on top the most current information.

*Question 2.* As everyone knows, we are currently negotiating another relief package that will potentially contain resources that could attract scammers. Are there steps that Congress, the FTC, or the states could take to proactively prevent future scams as the pandemic continues?

Answer. The FTC has already taken steps to warn consumers of potential scams that might accompany another relief package,<sup>19</sup> which have led to media reports and interviews. The FTC will continue to both monitor and forecast scammers’ activities that target both consumers and businesses—as it did early in the pandemic and around the first economic relief package.

Whenever the agency spots or anticipates scams, it alerts the public through its consumer and business blogs, which reach more than half a million people, including local media. It also does extensive outreach through and with partners, creates multimedia campaigns in multiple languages to share through social media, provides content for partner publications and activities, participates in webinars and

---

<sup>16</sup>See [FTC.gov/exploredata](https://www.ftc.gov/exploredata) for most up-to-date statistics about top reports related to COVID-19.

<sup>17</sup>See FTC Consumer Blog, *Cracking down on fake COVID-19 cures* (July 31, 2020), <https://www.consumer.ftc.gov/blog/2020/07/online-seller-failed-ship-next-day-ppe-promised-for-additional-tips>.

<sup>18</sup>See FTC Business Blog, *Protecting small businesses seeking financing during the pandemic* (Aug. 3, 2020), <https://www.ftc.gov/news-events/blogs/business-blog/2020/08/protecting-small-businesses-seeking-financing-during>.

<sup>19</sup>See FTC Consumer Blog, *Scams in between stimulus packages* (Aug. 11, 2020), <https://www.consumer.ftc.gov/blog/2020/08/scams-between-stimulus-packages>.

presentations (including with members of Congress), and carries out media interviews in English and Spanish.

It would be helpful for members to relay two key messages to constituents: sign up for the FTC's consumer and business alerts (at [www.ftc.gov/subscribe](http://www.ftc.gov/subscribe)), and be sure to report anything that might be a scam at [ftc.gov/complaint](http://ftc.gov/complaint). Reports help law enforcement spot trends, build cases, and develop consumer and business education that reflects what people are experiencing.

*Question 3.* How have the States and the FTC, along with the various Federal agencies, been working together to combat these scams?

Answer. The FTC has been actively coordinating with various government partners to combat COVID-19 scams. For example, the FTC has jointly issued numerous warning letters with several of its sister agencies, including the FDA, FCC, and the SBA. The FTC has also coordinated with state attorneys general to send simultaneous warning letters to targets located in their states. Some state attorneys general have brought enforcement actions against recipients of FTC warning letters located in their states. The FTC also participates in several working groups, attends regular meetings and coordinates efforts by sharing investigative leads.

In addition, the FTC has worked with Federal agencies such as the IRS, FEMA, GSA, and FDIC to coordinate consumer and business messaging and to deliver scores of webinars, presentations, social media shareables, and infographics about COVID-related scams. Moreover, recognizing the once-in-a-generation economic shift resulting from the pandemic, the FTC quickly developed and delivered materials on the financial impact of the coronavirus, including comprehensive PowerPoint presentations with talking points on issues like scams involving employment, mortgage relief, and student loan debt relief. FTC staff and partners, including Congressional offices, have used the PowerPoints to deliver presentations across the country.

---

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JERRY MORAN TO  
STU SJOUWERMAN

*Question 1.* With the noteworthy cybersecurity news related to Twitter last week serving as a significant example of social engineering, these types of attacks continue to evolve while posing increasing harm to Americans. Your testimony indicated that these types of threats are responsible for “upwards of 93 percent of data breaches.” Do you have any recommendations for this Subcommittee on how Congress can draw increased consumer attention to these risks or even prevent them from occurring in the first place?

Answer. E-mail continues to be the most common vector for launching social engineering attacks, with 99 percent of the actors being external to organizations. Most of these phishing and pretexting attacks are motivated by financial gain, however there is a substantial percentage which are motivated by corporate espionage.

The studies I referenced in my testimony make the point that phishing is relied on as the lead action or strategy of a more expanded attack, followed by malware installation and further actions to attain greater exfiltration of data.

Although 100 percent prevention of these attacks is not feasible, individuals and organizations can drastically reduce the success rate of bad actors by becoming more aware of how hackers operate and the concept of “social engineering.” The best way to draw attention to this problem is by creating programs which are designed to help potential victims become more aware. I believe to be more aware; one needs to face the fact that bad actors are trying to trick us. From there, individuals can learn to detect scams and then make appropriate decisions, like deleting and e-mail or not clicking a link.

*Question 2.* Your testimony highlighted the importance of ongoing security awareness training, which I would understand to be more than annual cybersecurity training required by some employers. How would you suggest employees and consumers alike to be proactive in their training efforts to prevent socially engineered cyber-attacks? What is the appropriate model and frequency for such training?

Answer. Given the advanced and dynamic models hackers use today, the static model of training is no longer adequate to protect employees, consumers, and organizations. To effectively equip employees and consumers with the ability to identify potential hacking attempts at the level they are now receiving, training must be equally dynamic.

The most effective and efficient models are those that train the individual, test their abilities, analyze success and failure, and then adapt future training, testing, and analysis to ensure the individual or organization is progressing. More importantly, consistent training allows the individual or organization to become more vigilant and sensitive to hacking attempts.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DAN SULLIVAN TO  
STU SJOUWERMAN

*Question 1.* We have seen various scams relating to this pandemic, including scams related to Federal relief efforts such as the PPP and economic impact payments (EIPs), as well as health-related scams that sell fake PPE and tout false cures and treatments for the virus. What do you believe is the most prevalent scam right now relating to the pandemic? And what should Americans and Alaskans most be on the lookout for to avoid it?

Answer. The latest data on COVID-related phishing scams from security researchers at CheckPoint comes with some good news and insightful trends that may help keep Americans secure.

We've seen just about every kind of COVID-related phishing scam over the last 5 months. From maps of the virus spread, to tracing apps, to class action lawsuits, to getting a tax rebate, and more—there seemed to be no end to the creativity of these scammers who find yet another way to use COVID as the draw to get potential victims to engage with malicious e-mail content.

According to CheckPoint, the good news is COVID-themed scams are on the decline—July saw a 50 percent decrease in the number of coronavirus-related attacks from the previous month. CheckPoint did find vaccine-related e-mail scams that take advantage of the world's race to find a vaccine.

The bad news is CheckPoint is still seeing a rise in all cyberattacks (including COVID attacks) which, according to their latest data, begin with a malicious phishing e-mail 80 percent of the time. Executables, Excel documents, and Word documents are the top three attachment types found in phishing scams.

While we're happy to see COVID-themed phishing e-mails go away sometime soon, there is no end in sight for the art of phishing. COVID merely played a viable long-term overarching theme for a wide range of scams. When COVID no longer gets people's attention and engagement, cybercriminals will turn to a new angle and story that will.

It's important to have users understand the need for vigilance when interacting with e-mail. Security Awareness Training provides users with ongoing education, teaching them what a suspicious or malicious e-mail looks like, what kinds of tactics and social engineering are used, and ways to avoid becoming a victim of a scam—COVID or otherwise.

*Question 2.* As everyone knows, we are currently negotiating another relief package that will potentially contain resources that could attract scammers. Are there steps that Congress, the FTC, or the states could take to proactively prevent future scams as the pandemic continues?

Answer. Broadly implementing the National Institute of Standards and Technology's (NIST) cybersecurity training guidelines is a good place to start. NIST highlights security awareness training as a core component of the "Protect" function of the cybersecurity framework. NIST recommends awareness and training for an organization's entire workforce and partners as a necessary defense against cyber attacks.

NIST Special Publication 800-50 provides guidelines for designing an employee awareness and training program, developing training materials and implementing a program. In Special Publication 800-50, NIST provides two clear objectives for security awareness and training: "Material should be developed with the following in mind: What behavior do we want to reinforce? (awareness); and What skill or skills do we want the audience to learn and apply? (training)."

NIST recommends training that includes educational, awareness-based content as well as skill development to help employees understand the threats they face and take the right action to prevent security incidents.

I believe an important additional step is to ensure dynamic training modules (rather than the old school annual PowerPoint presentation) and incorporate frequent social engineering testing into the NIST guidelines to ensure individuals and organizations remain vigilant and prepared to respond to new methods of attack that hackers will inevitably create to take advantage of future situations.

---

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JERRY MORAN TO  
LAURA MACCLEERY

*Question 1.* Your testimony described your work at the Center for Science in the Public Interest in identifying misleading consumer product claims for agencies like the FTC and FDA. Given your partnership with these agencies, do you have specific recommendations for Congress related to their available resources?

Answer. Congress can and should allocate significantly more resources to the FDA and FTC given that both agencies lack the resources necessary to adequately protect consumers during the pandemic, and more generally. The enforcement office with authority over supplements at FDA, for example, has only 6 FTEs, and is also responsible for enforcement over medical devices. That is simply insufficient to address the tide of misleading products and claims flooding the supplement marketplace.

Even prior to the pandemic, the FDA was badly outmaneuvered in a large and growing supplement marketplace with an estimated 50,000 or more products. Notably, increasing enforcement actually helps to improve the overall quality of the marketplace, as it would permit the agency to focus its resources on the worst actors, and to take more definitive steps to set enforcement precedents on a wide range of risky products.

In addition to resources, FDA should also be given greater authorities by Congress to act and address gaps in the oversight of supplements. Specifically, the Dietary Supplement Health and Education Act of 1994 (DSHEA) is in need of significant reforms to protect consumers. Because the FDA lacks the legal authorities, funding, and accountability to effectively oversee the safety of dietary supplement marketplace, Congress should:

- (1) Authorize state Attorney Generals to file civil enforcement actions against DSHEA violations, in coordination with the FDA and FTC. As many dietary supplement companies are small, fly-by night operations, it is difficult for one central agency to oversee the dietary supplement markets in all 50 states. State Attorney Generals can work with local health and law enforcement officials to identify supplements that pose local but significant threats to the safety of their residents.
- (2) Provide FDA with specific pre-market safety review authority and enhanced post-market surveillance of categories of supplements known to pose a heightened risk because they are commonly tainted with drugs or marketed to vulnerable populations (*e.g.*, weight-loss, sexual enhancement, and exercise supplements). Sponsors should be required to report all adverse reactions, not only the serious ones, as is the case at present.
- (3) Grant FDA the authority to require warning labels on products that interact with prescription or OTC medications. Many commonly consumed supplements have little-recognized adverse interactions with commonly taken medications. For example, St. John's Wort, a supplement that is believed by some to treat depression, menopausal symptoms, and smoking addiction (among other ailments) interacts with critical prescription medications, including blood thinners, anti-retroviral medications for HIV/AIDS, antidepressants, birth-control pills, some cancer medications, and other medications.
- (4) Recall authority over supplements tainted with prescription or other drugs. One gap in FDA's recall authority lies with supplements that are tainted with ingredients used in prescription drugs. These products fall within the meaning of the word "drug" under the FDCA and, therefore, fall outside of FDA's mandatory recall authority if they are not on the controlled substances list. (Currently, FDA has mandatory recall authority for food hazards, but not for drugs). To correct for this lack of enforcement power, FDA needs more robust recall authority over products tainted with drugs.
- (5) Criminal penalties for a failure to recall hazardous supplements subject to a recall notice. A study in *Journal of the American Medical Association (JAMA)* found that even when adulterated supplements were recalled, a majority of the recalled products on the shelves continued to contain banned adulterants. Criminal penalties for bad actors that ignore recalls and continue to sell dangerous supplements would provide stronger incentives for bad actors to remove those dangerous products.
- (6) Mandatory product registration requirements and requirements that retailers validate this registration (including online) to create transparency in the supply chain. Currently, it is impossible for the agency to know what supplements are currently on the market. By requiring product registration, the FDA can more closely monitor the claims and safety of supplements on the market. It will also make it easier for the agency to identify bad actors that attempt to circumvent oversight as both the agency and consumers would be able to tell if a particular supplement has registered with the FDA and is in compliance with FDA's safety standards.
- (7) To avoid the common problem that FDA is chasing multiple violations by the same company over similar products that differ mostly in its labeling, Con-

gress should allow the FDA to issue increased penalties for repeated violations when a letter has been issued but the product and company has been rebranded to avoid enforcement (*e.g.*, the FDA should be able to double the fines for the second offense, and triple it for the 3rd offense, etc.). The FDA should have the authority to enforce these penalties even when the product has been rebranded by the same seller or by the same company principals. The agency should also have the authority to determine when a company and product has been rebranded to avoid further enforcement and consider their continued sales of illegal supplements as a repeated violation subject to the escalating penalties. When determining if a company or product is rebranded to avoid enforcement, the FDA should be able to use factors such as similarities in the type of products, trade dress, ingredients, and ownership, and management.

*Question 2.* Your testimony noted that false and misleading claims were inevitable following the growth of the coronavirus into a global pandemic, which has been proven true. However, the FDA has been quickly on their heels so far, sending out hundreds of letters to those making false claims to withdraw them and take down their websites and products. The actions of the FDA appear to have a considerable impact in removing these products from the market or at least removing their false claims as they relate to treating the coronavirus. Is it your belief the FDA has not acted appropriately?

Answer. Our concern is not whether the FDA acted appropriately within their limited capabilities, but that the FDA does not have the tools necessary to combat the wide array of COVID-19 scams and health fraud in general, as described above. Unfortunately, health fraud is not a unique feature of COVID-19 but is common throughout the supplement industry and is a result of inadequate statutory authority, specific mandates, and funding.

Although the FDA, FTC, and private companies, such as Amazon, Google, and Twitter have made progress in eliminating many COVID-19 fraudulent claims, there are more COVID-19 supplements that persist, and many supplements continue to use illegal claims to profit from the pandemic. For example, although the FDA and Amazon have removed many COVID-19 claims from Amazon supplement listings, searches for COVID supplements, vitamins, or pills still yield hundreds of supplements with immunity boosting and illegal antiviral claims.

Furthermore, although many supplement companies have removed the terms COVID or coronavirus from their labeling, they continue to use their Web pages and social media profiles to promote their products as cures, treatments, and preventions for viruses more generally.

Finally, many of these fraudulent products that were and are currently marketed as COVID-19 cures were not developed during the pandemic or specifically developed for the coronavirus. These COVID-19 supplement scams are just a symptom of an ongoing problem. For example, although colloidal silver has been touted by scammers as treatment for COVID-19, it has been promoted as cures for numerous diseases decades before the pandemic. As the FDA has stated, “Unfortunately, during outbreak situations, fraudulent products claiming to prevent, treat or cure a disease almost always appear.” We have found products making fraudulent claims for opioid addiction treatment, tobacco addiction treatment, and female fertility treatment, in searches over the past few years. In the end, the COVID-19 pandemic has become just another opportunity for profiteers to market existing supplements that are not safe and effective for any disease or condition. Without fixing the underlying oversight problems, these same issues will continue to harm consumers and afflict the dietary supplement marketplace.

*Question 3.* You have recommended granting state attorneys general wider authority to enforce Federal statutes, do you have concerns about uneven efforts or capacity that may create a patchwork system of enforcement that leaves some states with a strict enforcement and others more lax?

Answer. It is true that companies who violate Federal law could be subject to different levels of enforcements in different states. However, a company would first have to break Federal law in order to be subjected to state enforcement, and any company within the U.S. remains bound by Federal law. The proposal would merely extend the effectiveness of these Federal provisions by encouraging state attorneys general to complement the efforts of resource-strapped Federal agencies.

Shared enforcement would also allow Federal agencies to focus their resources on the states that are more vulnerable to fraud. Currently, the FDA and FTC must oversee fraud under Federal statutes in every state. With shared enforcement, Federal agencies could work closely to enhance the effectiveness of states with greater capacity to enforce Federal statutes on their own to train them up, and then focus Federal efforts on states or regions with fewer resources.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DAN SULLIVAN TO  
LAURA MACCLEERY

*Question 1.* We have seen various scams relating to this pandemic, including scams related to Federal relief efforts such as the PPP and economic impact payments (EIPs), as well as health-related scams that sell fake PPE and tout false cures and treatments for the virus. What do you believe is the most prevalent scam right now relating to the pandemic? And what should Americans and Alaskans most be on the lookout for to avoid it?

Answer. In terms of dietary supplements, all American's should be on the lookout for supplements that claim to mitigate, treat, or prevent the effect of COVID-19. As Federal authorities have made clear, "[t]here are currently no medical products that are approved to treat or prevent COVID-19."

Yet supplement companies are preying on the fears of the public, looking for quick, low-cost ways of protecting themselves and their family. Unfortunately, consumers who buy ineffective supplements are throwing their money away and may be less likely to use proven means of prevention, such as masks and social distancing.

*Question 2.* As everyone knows, we are currently negotiating another relief package that will potentially contain resources that could attract scammers. Are there steps that Congress, the FTC, or the states could take to proactively prevent future scams as the pandemic continues?

Answer. The FDA and FTC should have dedicated resources from the Congress to help combat scams and predatory behavior that occur in a crisis such as this one. A COVID-19 scams funding stream to enlarge efforts to monitor the marketplace would be a strong step in that direction and could be dedicated to building more comprehensive surveillance and enforcement efforts by the agencies.

---

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JERRY MORAN TO  
THE U.S. FOOD & DRUG ADMINISTRATION

*Question 1.* Is there an estimate of how much money U.S. consumers have spent on these fraudulent products related to COVID-19?

Answer. The Food and Drug Administration (FDA or the Agency) plays an essential role in overseeing our Nation's medical products as part of our vital mission to protect and promote public health, including during public health emergencies. The Agency is an active partner in the Novel Coronavirus (COVID-19) response, working closely with our government and public health partners across the Department of Health and Human Services, as well as with our international counterparts. Our work is multifaceted, focusing on actively facilitating efforts to diagnose, treat and prevent the disease; surveilling the medical product supply chain for potential shortages or disruptions and helping to mitigate such impacts, as necessary; and leveraging the full breadth of our public health tools as we oversee the safety and quality of FDA-regulated products for American patients and consumers.

Within FDA, several parts of the Agency are involved in combating health fraud. The Office of Criminal Investigations, Office of Enforcement and Import Operations, and Health Fraud Branch within the Agency's Office of Regulatory Affairs all work collaboratively with colleagues in FDA's product centers and the Office of Chief Counsel. FDA also works closely with other government agencies including the Centers for Disease Control and Prevention (CDC), U.S. Customs and Border Protection, the Federal Trade Commission, and the U.S. Department of Justice.

FDA has established a cross-agency task force dedicated to closely monitoring for unproven products sold with false or misleading COVID-19 claims. We have reached out to major retailers to ask for their help in monitoring their online marketplaces for fraudulent coronavirus products. Products may be subject to FDA investigation and potential enforcement action if they are sold or distributed with claims to prevent, treat, or cure COVID-19 and have not been approved, cleared, or authorized by the Agency for that intended use. Our task force has already alerted retailers that their platforms included listings for fraudulent COVID-19 products online, and several retailers have responded that they plan to monitor for false or misleading COVID-19 claims.

In addition, FDA's website includes a dedicated web page alerting consumers to beware of fraudulent coronavirus tests, vaccines, and treatments,<sup>1</sup> and advising con-

---

<sup>1</sup> <https://www.fda.gov/consumers/consumer-updates/beware-fraudulent-coronavirus-tests-vaccines-and-treatments>

sumers and health care professionals that they can report suspected fraud to the Agency's Health Fraud Program<sup>2</sup> or Office of Criminal Investigations.<sup>3</sup>

FDA is committed to taking action to prevent unscrupulous actors from selling fraudulent products related to this outbreak; however, the Agency does not routinely collect data on the amount of money that U.S. consumers have spent on fraudulent products related to COVID-19, and is unable to provide such an estimate.

*Question 2.* Do you have an estimate as to how many hospitalizations have resulted from the use of these fraudulent products?

Answer. FDA does not routinely collect national hospitalization data and is unable to provide such an estimate. However, the Agency works closely with CDC and state health departments, utilizes the Agency's MedWatch Adverse Event Reporting program, which includes health care professional and consumer complaints, to help identify products that may be causing injury or death, and takes appropriate action to protect the public health. This is particularly true when the injuries caused are serious enough to warrant medical treatment or hospitalizations.

For example, earlier this year FDA identified certain hand sanitizer products that tested positive for contamination with methanol, a substance often used to create fuel and antifreeze. Methanol is not an acceptable active ingredient for hand sanitizer products, and can be toxic when absorbed through the skin as well as life-threatening when ingested. State officials also reported adverse events, including blindness, hospitalizations and death, in people that had ingested methanol-contaminated hand sanitizers. FDA quickly took action to warn consumers about methanol-contaminated and other potentially dangerous hand sanitizer products and encouraged health care professionals, consumers and patients to report adverse events to the Agency's MedWatch Adverse Event Reporting program. We worked proactively with manufacturers to recall these products, and encouraged retailers to remove them from store shelves and online marketplaces; in addition, FDA took action to help prevent certain hand sanitizers from entering the United States by placing them on an import alert.

*Question 3.* Has the COVID-19 Fraud Task Force examined the Deep Web for other, more persistent producers or sellers?

Answer. FDA has received thousands of complaints from U.S. consumers about unproven cures and illegitimate test kits being offered for sale on the internet, and the Agency identified tens of thousands of new "high-risk" Internet domain names that were registered in early 2020. To proactively identify and neutralize these threats to consumers, the Agency launched "Operation Quack Hack" in March 2020.

Operation Quack Hack leverages Agency expertise and advanced analytics to protect consumers from fraudulent FDA-regulated products during the COVID-19 pandemic. Building on our previous experience with illegal online pharmacies, a team of consumer safety officers, special agents and intelligence analysts triage incoming complaints about fraudulent and unproven products sold for prevention, diagnosis, or treatment of COVID-19. Where appropriate, complaints are sent to other agencies or to FDA centers for additional review, and may be referred for a warning letter, civil action, or criminal investigation.

In some cases, following a preliminary investigation, the Operation Quack Hack team sends an abuse complaint to the domain name registrars or a report to online marketplaces. These abuse complaints and reports are intended to notify online entities that their platforms were being used to sell an unapproved, unauthorized, or uncleared medical product during the COVID-19 pandemic.

The Operation Quack Hack team has reviewed thousands of websites, social media posts, and online marketplace listings, resulting in more than 110 warning letters to sellers, more than 220 reports sent to online marketplaces, and more than 270 abuse complaints sent to domain registrars. These initiatives have led domain registrars to review and take down numerous websites illegally selling unproven products.

ORA's Office of Criminal Investigations has discovered Dark Websites purporting to sell a range of COVID-19 related medical products such as convalescent plasma, vaccines, drugs, and personal protective equipment (PPE). Many of the sites appear to be associated with "non-delivery" fraud schemes involving PPE, medical equipment such as ventilators, and other supplies or equipment in short supply during the current COVID-19 pandemic. "Non-delivery of merchandise" is a scheme in which a seller on an Internet website (including auction websites) accepts payment

<sup>2</sup><https://www.fda.gov/safety/report-problem-fda/reporting-unlawful-sales-medical-products-internet>

<sup>3</sup><https://www.accessdata.fda.gov/scripts/e-mail/oc/oci/contact.cfm>

for an item yet intentionally fails to ship it. Sellers like these sometimes will re-list the item and attempt to sell it again through a different user name.

FDA will continue to monitor social media and online marketplaces for listings promoting and selling fraudulent products to prevent, diagnose, cure, or treat COVID-19. We have been working with retailers to remove fraudulent products from store shelves and online, and we are also increasing our enforcement at ports of entry to ensure that fraudulent products do not enter the country through our borders. Americans expect and deserve treatments that are safe, effective and meet appropriate standards, and FDA will continue its efforts to protect consumers from those who place profits above the public health during this pandemic.

