STAYING A STEP AHEAD: FIGHTING BACK AGAINST SCAMS USED TO DEFRAUD AMERICANS

HEARING
BEFORE THE
SUBCOMMITTEE ON CONSUMER PROTECTION, PRODUCT SAFETY, INSURANCE, AND DATA SECURITY
OF THE
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION
UNITED STATES SENATE
ONE HUNDRED FIFTEENTH CONGRESS
FIRST SESSION
MARCH 21, 2017

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

<table>
<thead>
<tr>
<th>Hearing held on March 21, 2017</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Statement of Senator Moran</td>
<td>1</td>
</tr>
<tr>
<td>Statement of Senator Blumenthal</td>
<td>2</td>
</tr>
<tr>
<td>Statement of Senator Thune</td>
<td>26</td>
</tr>
<tr>
<td>Statement of Senator Inhofe</td>
<td>28</td>
</tr>
<tr>
<td>Statement of Senator Udall</td>
<td>30</td>
</tr>
<tr>
<td>Statement of Senator Cortez Masto</td>
<td>32</td>
</tr>
<tr>
<td>Statement of Senator Hassan</td>
<td>34</td>
</tr>
<tr>
<td>Statement of Senator Klobuchar</td>
<td>36</td>
</tr>
<tr>
<td>Statement of Senator Markey</td>
<td>38</td>
</tr>
</tbody>
</table>

## WITNESSES

| Pre pared statement                                                                              | 6    |
| Hon. Terrell McSweeney, Commissioner Federal Trade Commission                                   | 7    |
| Pre pared statement                                                                              | 9    |
| Hon. Mike DeWine, Ohio Attorney General                                                            | 10   |
| Pre pared statement                                                                              | 12   |
| Frank Abagnale, Author and Consultant, Abagnale & Associates                                      | 15   |
| Pre pared statement                                                                              | 17   |
| Mike Schwanke, Reporter, KWCH-12 Eyewitness News                                                | 18   |
| Pre pared statement                                                                              | 20   |

## APPENDIX

| Letter dated March 17, 2017 to Hon. Deb Fischer from Scott Merritt, Executive Director, Nebraska Hotel & Lodging Association | 47   |
| Response to written questions submitted to Hon. Maureen K. Ohlhausen by:                         |      |
| Hon. John Thune                                                                                  | 51   |
| Hon. Deb Fischer                                                                                 | 56   |
| Hon. Jerry Moran                                                                                 | 57   |
| Hon. Dean Heller                                                                                 | 61   |
| Hon. Todd Young                                                                                  | 62   |
| Hon. Bill Nelson                                                                                 | 63   |
| Hon. Richard Blumenthal                                                                          | 64   |
| Hon. Amy Klobuchar                                                                               | 66   |
| Response to written questions submitted to Hon. Terrell McSweeney by:                           |      |
| Hon. Jerry Moran                                                                                 | 67   |
| Hon. Dean Heller                                                                                 | 69   |
| Hon. Todd Young                                                                                  | 70   |
| Hon. Bill Nelson                                                                                 | 70   |
| Hon. Richard Blumenthal                                                                          | 70   |
| Response to written questions submitted to Hon. Mike DeWine by:                                 |      |
| Hon. Jerry Moran                                                                                 | 72   |
| Hon. Todd Young                                                                                  | 72   |
| Hon. Bill Nelson                                                                                 | 73   |
| Hon. Richard Blumenthal                                                                          | 73   |
| Response to written questions submitted to Frank W. Abagnale, Jr. by:                           |      |
| Hon. Bill Nelson                                                                                 | 73   |
| Hon. Richard Blumenthal                                                                          | 74   |
| Response to written question submitted by Hon. Richard Blumenthal to:                           |      |
| Mike Schwanke                                                                                   | 75   |
STAYING A STEP AHEAD: FIGHTING BACK AGAINST SCAMS USED TO DEFRAUD AMERICANS

TUESDAY, MARCH 21, 2017

U.S. Senate,

The Subcommittee met, pursuant to notice, at 2:33 p.m. in Room SR–253, Russell Senate Office Building, Hon. Jerry Moran, Chairman of the Subcommittee, presiding.

Present: Senators Moran [presiding], Blumenthal, Inhofe, Young, Klobuchar, Markey, Booker, Udall, Hassan, Cortez Masto, and Thune.

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

The Chairman. The committee will come to order. Good afternoon, and welcome to our first hearing of this Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security, in this new Congress. I’m pleased that Ranking Member Blumenthal is here today. He has an especially busy schedule as a member of the Senate Judiciary Committee. And I look forward to working with him not only on this hearing, but throughout this Congress, as we try to address issues that are facing consumers and overseeing the work of the Federal consumer protection agencies that fall within this subcommittee’s jurisdiction.

I am convening this hearing to discuss scams affecting American consumers. In the Commerce Committee, we often debate, and sometimes differ on, the proper role of government, the appropriate level of regulation, and the best way to protect the public without imposing unnecessary burdens on the private sector that would stifle their contribution to the economy.

Today, however, the issue before the Committee is one on which there is broad consensus. Consumers need protection from those who seek to defraud them through scams, and the Federal Government must do everything it can to protect consumers from truly bad actors. American citizens are scammed out of billions upon billions of dollars every year with zero corresponding benefit to our Nation’s economy. With technology becoming more sophisticated, so also has the complexity of scams continued to make this circumstance even more difficult. From fake charity donation solicita-
tions calls, to phishing e-mail scams that lead to identity theft, a wide variety of scams that unduly harm Americans continue to bypass consumer protection enforcement measures at the Federal, state, and local levels.

To that end, this committee oversees the Federal Trade Commission, and I am pleased that we are joined today by Acting Chairman Ohlhausen and Commissioner McSweeny, who together constitute the current FTC in its entirety.

However, with all due respect to Chairman Ohlhausen and Commissioner McSweeny, I believe it’s important that the President act swiftly to restore the Commission to its full strength. The FTC’s work in support of consumers and competition is too important for an agency to continue operating shorthanded in weeks and months ahead.

I would also like to extend a welcome to our former colleague, Ohio Attorney General Mike DeWine, Frank Abagnale, and Mr. Mike Schwanke. All three will provide unique perspectives today reflecting ways government protects citizens through fraud prevention, the perspectives of scam victims, and the mentality and common tactics of the scammers themselves.

This is a wonderful witness panel for today's hearing, which I hope will have a meaningful impact to raise awareness about this important issue, educate consumers about particular scams to watch for, and prevent future scams from continuing to harm consumers acting as a significant drag on our economy and all the personal challenges a scam creates.

Thank you all for being here. And I turn now to the Ranking Member for his opening statement.

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

Senator Blumenthal. I join the Chairman in thanking you for being here. It is a great panel. And I want to thank the Chairman for holding this important hearing so that we and the consumers of America can stay one step ahead of scams, which have become so ubiquitous and threatening in our modern, technologically-driven life.

Scams are a real hardship for individuals, but they’re also a scourge on our economy, unfairly victimizing consumers, compromising our trust in the marketplace, and siphoning millions of dollars from individuals and legitimate, honest businesses—not just individual consumers, but also businesses who suffer as a result of scams. In fact, the FTC has secured $14 billion in consumer relief since Fiscal Year 2014 alone.

I am pleased that our former colleague, as Attorney General, Mr. DeWine is here with us, and that I am joined by two former Attorneys General on the panel today. And we know how pervasive these frauds are, not just the classic wire fraud schemes, but also the telephone technician scams targeting small and medium-sized businesses.

The type of scheme is as endless as the human imagination and often as frustrating as a Whack-A-Mole game; you shut one scam down and dozens more arise. That’s why informed consumers are one of the most powerful tools we have, because the best preven-
tion is consumer education and care and self-protection. But we also need swifter enforcement, and severe and appropriate punishment, to effectively deter bad actors and to ensure that any company complicit in a scam doesn’t simply write off a fine or a government lawsuit as the cost of doing business. My hope is that we will talk about stronger punishments against individuals so as to deter these scams and close some of the gaping holes in our present law.

First, we ought to make sure that we’re pursuing enforcement actions against any and all aiders and abettors of fraud. Search engines, social media sites, and online generators ought to be on notice that they have a duty to implement checks to make sure that they are not complicit in connecting consumers to illegitimate businesses intent on fleecing people’s pocketbooks.

Second, the FTC is currently limited in its ability to pursue cases against nonprofits. Considering that the nonprofit sector is estimated to account for 5 percent of the Nation’s GDP and 10 percent of the private sector workforce, there is also the vulnerability to fraud on the nonprofit side, and we’ve seen it occur in this sector.

Third, in order to more effectively deter unlawful schemes, we ought to strengthen the FTC’s ability to seek civil penalties on first violations of Section 5.

And fourth, the FTC shouldn’t just go after bad guys once they’ve already left a slew of victims in their wake; the FTC also ought to have the ability to set rules in appropriate circumstances that stop the bad behavior in the first place before consumers are harmed.

Finally, there is no denying, no getting around the fact, that the hiring freeze has had consequences for the FTC, in effect inhibiting its ability to effectively crack down on fraud and protect consumers. And the recent actions, including the budget proposal that cuts government spending on enforcement efforts, can only have further bad consequences.

I would also like to say a word about how Congress is on the verge of using the Congressional Review Act to rescind the Federal Communication Commission’s broadband privacy rules. Republican colleagues say they want to transfer privacy oversight of broadband back to the FTC, but the FTC doesn’t have jurisdiction over security and privacy practice of broadband, cable, and wireless carriers in their capacity as common carriers.

And if the Ninth Circuit’s recent decision on FTC v. AT&T adopting a status-based instead of activity-based interpretation of the FTC’s common carrier exemption is upheld, the FTC’s jurisdiction and ability to improve privacy and security obligations would be even further curtailed. The elimination of the FCC’s rules would result in a yawning chasm where broadband and cable companies have no discernable regulation. That outcome would be devastating for consumers.

My hope is that this committee, like the FTC, can continue working on a bipartisan basis, and I look forward to passing legislation like the Better Online Ticket Sales Act and the Consumer Freedom Review Act, as we did in the 114th Congress, that give the FTC additional authority to protect consumers. Thank you all for being here today.

The CHAIRMAN. Senator, thank you very much. We welcome our panel of witnesses and thank them for their testimony. Our wit-
nesses are the Honorable Maureen K. Ohlhausen, Acting Chairman of the Federal Trade Commission; the Honorable Terrell McSweeny, Commissioner of the Federal Trade Commission; the Honorable Mike DeWine, Attorney General of the State of Ohio; and I would turn to the gentleman from Oklahoma to introduce someone he claims is an Oklahoman.

[Laughter.]

The CHAIRMAN. But do ask him where his children went; to what university.

[Laughter.]

Senator INHOFE. Well, they couldn't help that they couldn't get in.

[Laughter.]

Senator INHOFE. Well, I'm just delighted to have Frank Abagnale here. And I'm very, very proud that he did raise a family in Oklahoma, and I see him on the plane all the time going back and forth. And I'm anxious to ask you the first question, but I won't do that until it's my turn.

Mr. Abagnale, thank you for accepting the invitation to testify before the Committee on the subject of fighting back against scams used to defraud Americans. Your perspective, as your life history, is unique among the witnesses. After your teenage years, you were made notorious by the movie "Catch Me If You Can," which I just saw, and I'm just really excited about that. I know you in a different way than I have in the past. But, anyway, we're looking forward to your unique perspective that we'll enjoy very much.

For over 40 years, financial institutions, corporations, and government agencies, including the Federal Bureau of Investigation, have benefited from your expertise in fraud-related crime. Because of you, countless Americans are better protected from scams because of their education and heightened awareness that you provide. The FBI has more than a generation of agents taught to detect, track, and solve fraud-related crimes against Americans. In recognition of fraud that is happening more and more online, you became AARP's Fraud Watch Network Ambassador to educate consumers about the way to protect themselves from identity, and I think you had one just the other day in Oklahoma, such a meeting.

So we look forward to your testimony this afternoon as we explore the challenges to educating and protecting Americans from fraud as well as the steps we can take to educate and empower those fighting against it. Welcome to you.

Mr. ABAGNALE. Thank you, Senator.

The CHAIRMAN. I'm not as constrained as the Senator from Oklahoma is. Your children went to what university?

Mr. ABAGNALE. I have two sons who graduated from KU.

The CHAIRMAN. Thank you. Our final witness on this panel is Mr. Mike Schwanke, of KWCH, the CBS affiliate in Wichita, Kansas, an investigative reporter.

Let us begin with the testimony of the Chairwoman, and we'll work our way to my right, to her left.

Welcome.
Commissioner OHLHAUSEN. Thank you. Chairman Moran, Ranking Member Blumenthal, and members of the Subcommittee, I am pleased to appear before you today alongside my colleague, Commissioner Terrell McSweeny, and the other panelists to discuss the importance of combating consumer fraud.

Protecting American consumers involves several factors, including market forces, private rights, and public law enforcement. The first factor is a competitive marketplace in which consumers have adequate information and a variety of choices. In these circumstances, most companies will care about their reputation and their ability to attract repeat customers. Companies therefore have incentives to be honest and keep the promises they make to consumers or else lose out to their competitors.

The second factor is private legal rights as well as effective mechanisms to enforce those rights. The ability of consumers to bring legal action to enforce their rights in the face of, for example, a breach of contract is an important protection for consumers.

The third factor is public law enforcement by the FTC, state attorneys general, and other entities. This is necessary in instances when a competitive marketplace and private litigation are not enough to protect consumers. A prime example of this is the subject of today’s hearing, consumer fraud. A fraudster is often immune to market forces because it doesn’t care about its reputation or attracting repeat customers. In addition, fraudsters will typically take steps to avoid detection of their scams or to dissipate assets, making it difficult for consumers to vindicate their rights in the court system.

Many consumers are thus left without a viable recourse against fraudulent practices. In these circumstances, the FTC, as the Nation’s primary consumer protection agency, must step in. And as Acting Chairman, I’ve instructed Commission staff to focus our law enforcement efforts on stopping fraudulent practices, particularly those that are causing the largest consumer harm. In doing so, we’ll ensure that the Commission is using its resources for the maximum benefit of consumers.

And I would like to touch briefly today on two populations in particular, military consumers and small businesses.

Military consumers are an attractive target for fraudsters. They receive a regular paycheck, change addresses frequently, and belong to a close-knit community. In Calendar Year 2016, the FTC’s Consumer Sentinel Network database received over 103,000 complaints from military and veteran consumers, the vast majority of which were about imposter scams, identity theft, and other frauds. Protecting those consumers who are protecting our country is of paramount importance, but clearly there is still work yet to do.

Small businesses are also attractive targets for fraud. The Better Business Bureau reports that thousands of small businesses are the targets of scams each year. Fraudsters often take advantage of the fact that small businesses lack a sophisticated recordkeeping system and thus are more susceptible to fake invoices, phishing attacks, and marketing scams. Frauds targeting small businesses,

many of which are scrambling just to make ends meet, can have a stifling effect on innovation and competition in the marketplace.

The Commission also actively works to help consumers recognize frauds before they fall victim. The Commission produces websites, brochures, and other materials to educate the public on common scams and how to avoid them. Often these materials are geared toward frequently targeted groups, such as seniors, Spanish speakers, and the two groups I mentioned, military consumers and small businesses.

For example, we have a website, Military.Consumer.gov, devoted to educating military consumers about fraud issues. And I’ve also directed Commission staff to create a webpage for small businesses on which we will provide a one-stop shop for all of our guidance to small business on how to avoid scams. And I invite the Subcommittee to consider linking to our materials for the benefit of your constituents.

Now, I’m proud of the work the FTC has done to combat fraud, but we can’t become complacent or distracted from that core mission. Fraudsters are always thinking up new scams, and the Commission must be and will be at the forefront of protecting American consumers.

So thank you for your time, and I look forward to the discussion.

[The prepared statement of Ms. Ohlhausen follows:]

PREPARED STATEMENT OF HON. MAUREEN K. OHLAUSEN, ACTING CHAIRMAN, FEDERAL TRADE COMMISSION

Chairman Moran, Ranking Member Blumenthal, and members of the Subcommittee, I am pleased to appear before you today alongside my colleague Commissioner Terrell McSweeney and the other panelists to discuss the importance of combatting consumer fraud.

Protecting America’s consumers involves several factors, including market forces, private rights, and public law enforcement. 1

The first factor is a competitive marketplace in which consumers have adequate information and a variety of choices. In these circumstances, most companies will care about their reputation and their ability to attract repeat customers. Companies will therefore have incentives to be honest and keep the promises they make to consumers or else lose out to their competitors.

The second factor is private legal rights, as well as effective mechanisms to enforce those rights. The ability of consumers to bring legal action to enforce their rights in the face of, for example, a breach of contract is an important protection for consumers.

The third factor is public law enforcement by the FTC, state Attorneys General, and other entities. This is necessary in instances when a competitive marketplace and private litigation are not enough to protect consumers. A prime example of this is the subject of today’s hearing: consumer fraud. A fraudster is often immune to market forces because it does not care about its reputation or attracting repeat customers. In addition, fraudsters will typically take steps to avoid detection of their scams or to dissipate assets making it difficult for consumers to vindicate their rights in the court system.

Many consumers are thus left without a viable recourse against fraudulent practices. In these circumstances, the FTC, as the Nation’s primary consumer protection agency, must step in. As Acting Chairman, I have instructed Commission staff to focus our law enforcement efforts on stopping fraudulent practices, particularly those that are causing the largest consumer harm. Doing so will ensure that the Commission is using its resources for the maximum benefit of consumers.

---

I would like to touch briefly today on two populations in particular: military consumers and small businesses.

Military consumers are an attractive target for fraudsters. They receive a regular paycheck, change addresses frequently, and belong to a close-knit community. In calendar year 2016, the FTC’s Consumer Sentinel Network database received over 103,000 complaints from military and veteran consumers, the vast majority of which were about imposter scams, identity theft, and other frauds. Protecting those consumers who are protecting our country is of paramount importance, but clearly there is still work yet to do.

Small businesses are also attractive targets for fraud. The Better Business Bureau reports that thousands of small businesses are the targets of scams each year. Fraudsters often take advantage of the fact that many small businesses lack a sophisticated recordkeeping system and are thus more susceptible to fake invoices, phishing attacks, and marketing scams. Frauds targeting small businesses, many of which are scrambling just to make ends meet, can have a stifling effect on innovation and competition in the marketplace.

The Commission also actively works to help consumers recognize frauds before they fall victim. The Commission produces websites, brochures, and other materials to educate the public on common scams and how to avoid them. Often, these materials are geared towards frequently targeted groups, such as seniors, Spanish-speakers, and the two groups I mentioned: military consumers and small businesses. For example, we have a website, military.consumer.gov, devoted to educating military consumers about consumer fraud issues. I have also directed Commission staff to create a webpage for small businesses on which we will provide a one-stop shop for all of our guidance to small businesses on how to avoid scams. I invite the Subcommittee to consider linking to our materials for the benefit of your constituents.

I am proud of the work the FTC has done to combat fraud, but we cannot become complacent or distracted from that core mission. Fraudsters are always thinking up new scams, and the Commission must be and will be at the forefront of protecting America’s consumers. Thank you and I look forward to your questions.
tion estimated that 10.8 percent of all Americans over the age of 18, or more than 25 million people, had been the victim of a fraud.

The growth in imposter scam complaints is particularly striking. They surpass the number of identity theft complaints for the first time ever last year. In imposter scams, someone poses as a friend, family member, romantic interest, legitimate company, or even a government agency in order to obtain money or personal information from the victim. Government imposter scams, the most common type of imposter scam reported last year, run the gamut from callers claiming to be from the IRS and demanding payment of back taxes to debt collectors claiming to be from a law enforcement agency.

Other imposters purport to be calling on behalf of a company, such as Microsoft or Apple. They convince consumers that their computers are infected with malware. In reality, no such virus exists, but consumers pay for costly technical support services with very little, if any, value at all.

We are taking action to stop these scams at the FTC. Last year, we brought multiple cases against tech support scams as well as action against an entity that was impersonating the Department of Transportation. Stopping fraud, as Acting Chairman Ohlhausen has said, is a core FTC priority. This includes not just pursuing bad actors, who directly perpetuate the frauds, but also others who facilitate those scams.

One example is our recent case against Western Union, which paid $586 million to settle charges that it failed to stop scammers from using its money transfer system to collect payments for numerous types of fraud, including many of the types of scams that we are talking about today.

Protecting consumers is just too big a job for the FTC to do alone, and that's why we partner with other government agencies, states, state attorney generals, and civic organizations in our anti-fraud work. And that is also why we invest heavily in consumer and business education.

Educating American consumers is one of the best ways we can combat fraud. We produce materials in multiple languages for almost every demographic and make them available across all platforms to reach the broadest possible audience. We hold Ethnic Media Roundtables around the country to help diverse communities highlight frauds that are specifically affecting them.

We also have a campaign to help older people learn about common scams and pass that information on to their peers. And we work closely with the Department of Defense and others to help the military community avoid frauds.

It is vital that we continue this important outreach and ensure that we have sufficient resources to meet the demands for our materials. This is particularly true—and I am biased in this regard as a parent—for our educational materials for parents and children, which help parents keep their kids safe online. These materials need to be updated to remain relevant, including optimizing them for mobile platforms.

The FTC must continue to stay abreast of emerging consumer protection issues. In our always-on, always-connected digital world, which is so full of marvelous innovations, we also have new oppor-
tunities for fraudsters and bad actors. Imposter scams are just one example of that trend.

I am particularly concerned, for example, about the growth in ransomware attacks. Ransomware attacks on computers, both for individuals and businesses, are unfortunately already well known. But I worry that attacks on connected consumer devices will soon become more common, especially given wide-ranging industry data security practices. In the not-too-distant future, a consumer might turn on her smart TV only to see a message asking for $50 in Bitcoin if she wants to watch television again.

In the world of cyber threats, the FTC must keep pace with changing technology, and we've been doing that by engaging with stakeholders and, most importantly, bringing technologists into our work. The FTC's Office of Technology Research and Investigation, or OTech, is in its second year, and I am pleased that our talented interdisciplinary team of lawyers and computer scientists is continuing to provide important in-house capabilities supporting our mission.

As our complaint data indicates, scammers are finding creative new ways to target consumers, so it is vital that the FTC continue to have proper resources to keep pace with them. As we'll discuss today, our consumer protection mission has a big impact on people's lives. Last year alone, we obtained orders that will return more than $11 billion directly to consumers in the form of redress. That's more than 35 times our annual operating budget. Our enforcement actions not only provide American consumers with justice, they help strengthen consumer trust in the marketplace, strengthening the dynamism of the American economy itself.

So thank you again for your attention and for holding this hearing.

[The prepared statement of Commissioner McSweeny follows:]
We are taking action to stop these scams. Last year we brought multiple cases against tech support scams, as well as an action against an entity that was impersonating the Department of Transportation.

Stopping fraud is a core FTC priority. This includes not just pursuing bad actors who are directly perpetrating the frauds, but also others whose facilitate scams. One example is our recent case against Western Union, which paid $586 million to settle charges that it failed to stop scammers from using its money transfer system to collect payments for numerous types of fraud.

Protecting consumers is too big a job for the FTC to do alone. That's why we partner with other government agencies, states, and civic organizations in our anti-fraud work—and why we invest in consumer and business education.

Educating American consumers is one of the best ways we can combat fraud. We produce materials in multiple languages for almost every demographic and make them available across platforms to reach the broadest possible audience. We hold Ethnic Media Roundtables around the country to help diverse communities highlight frauds affecting them.

We also have a campaign to help older people learn about common scams and pass that information on to their peers. And we work closely with the Department of Defense and others to help the military community avoid fraud.

It is vital that we continue this important outreach—and ensure that we have the resources to meet the demand for our materials. This is especially true for our educational materials for parents and children, which help parents keep their kids safe online. It's critical that we keep these materials relevant and up to date, including optimizing them for mobile platforms.

The FTC must continue to stay abreast of emerging consumer protection issues. Our always-on, always-connected digital world is full of marvelous innovations—but it also creates some new opportunities for bad actors.

I'm particularly concerned about the growth in ransomware attacks. Ransomware attacks on computers—both for individuals and businesses—are unfortunately already well known. But I worry that attacks on connected consumer devices will soon become more common—especially given wide-ranging industry data security practices. In the not-too-distant future a consumer might turn on her smart TV only to see a message that asks for $50 in Bitcoin if she wants to watch television again.

In a world of new cyber threats, the FTC must keep pace with changing technology. We have been doing that by engaging with stakeholders—and, most importantly, bringing technologists on board. The FTC's Office of Technology Research and Investigation, or OTech, is in its second year.

OTech is a talented inter-disciplinary team of lawyers and computer scientists who provide us with in-house research capabilities and the expertise to understand cutting-edge technology—like cross-device tracking, or how algorithms impact consumer choice. As more of these technologies come into the marketplace, it is vital that the FTC continue to expand these capabilities.

Unlike many other enforcement agencies, the Federal Trade Commission sends refund checks to individual consumers who are harmed by unfair and deceptive business practices. Last year, we obtained orders that will return more than $11 billion in redress to consumers.

Our enforcement actions not only provide American consumers with justice, they help to strengthen consumer trust in the marketplace, strengthening the dynamism of the American economy itself.

Thank you again for holding this hearing. I look forward to answering your questions.

The CHAIRMAN. Mr. Attorney General.

STATEMENT OF HON. MIKE DeWINE,
OHIO ATTORNEY GENERAL

Mr. DeWine, Mr. Chairman, Chairman Moran, thank you very much for inviting us to be here today, and Ranking Member Blumenthal, and all the members of the Committee.

You know, we've always had—I suppose time immemorial we've had con artists and crooks, swindlers, but what is really different today is they now have a very long arm, and, of course, that long arm is the Internet and long-distance telephone. The Internet and social media have really transformed the world we live in, and in some cases, for very, very good ways, FaceTime with one of your
grandchildren, something that my wife, Fran, and I enjoy. But, unfortunately, scammers also use these modern conveniences to commit fraud and to satisfy their greed.

Now, grandparent scams are one of the most frequently reported and the most, I think, gut-wrenching scams that my office receives. Fran and I have 8 children and 22 grandchildren, and like all grandparents, there is nothing, nothing, we would not do for our grandkids, and that is exactly the mentality that the scammers prey upon. There is a reason they call grandparents and they don't call parents.

The scam often begins with a phone call telling grandparents that one of their grandchildren has been in a car accident, caught with drugs, or put in jail. The caller pretends either to be the grandchild or an attorney or a law enforcement officer, and tells the grandparent to send money immediately to have the charges dismissed, to cover court costs, or to allow the grandchild to return home.

As part of the scheme, grandparents often are instructed not to talk to other people. In fact, that's normally what the call is all about. They say, “Grandpa, this is Sara.” “Where are you, Sara? I thought you were at Miami University.” “No, Grandpa, I'm so-and-so.” And then, “Do your parents know that?” “Don’t tell my parents.” And that’s always what they say. Many times the grandparents not only pay once, but they pay several different times, sometimes for attorneys’ fees or other unexpected costs. Eventually the grandparents discover that their grandchild was not truly in trouble, but by then, of course, it is much too late. The average loss to an individual Ohioan that's been reported to us for this specific scam is over $5,000.

Another popular scam is the romance scam. In a typical romance scam, the con artist meets the victim online through a dating or social networking site. The scammer often claims to live in the United States, but says he or she is temporarily located overseas due to a military assignment, business trip, or other reason. Eventually, he or she asks the victim to send money to help cover some type of cost, such as airfare to visit the victim, medical expenses, or fees associated with military leave. Not surprisingly, once the money is sent, it’s nearly impossible for anyone to recover. The average loss from this particular scam in the state of Ohio is over $26,000.

As Attorney General, I've been committed to treating these scams as what they are, and that is crimes. Shortly after becoming Attorney General, I established an Economic Crimes Unit in my Consumer Protection Section. The unit includes seasoned prosecutors and investigators who are tasked with holding these fraudsters accountable and assisting local law enforcement and prosecutors in identifying, investigating, and prosecuting consumer fraud of a criminal nature.

One of the reasons our Economic Crime Unit has been successful is that we're able to see patterns of conduct occurring across multiple jurisdiction lines, across multiple counties. We can then make connections with law enforcement and victims and show the true scope of the criminal enterprise.
I think, Mr. Chairman and members of the Committee, that we need to apply that same logic to scams and economic crimes nationwide on the Federal level. To be successful, we need to break down barriers to communication. We need to have more sharing of information and resources, and we need to work together to combat crime on the national and the international level.

We’ve all heard about the lottery scam, “You’ve won the lottery.” We’ve seen that model, though, of catching these people work in what’s called Project JOLT, where the U.S. Department of Homeland Security has partnered with a Jamaican police force, industry, and other law enforcement agencies to take down Jamaican lottery scammers, a number of whom have recently been extradited to the United States to face Federal charges.

Mr. Chairman and members of the Committee, now is the time to apply those lessons to other scams and crimes because, simply put, there is strength in numbers. When multiple agencies put their resources, their intelligence, their ingenuity together, great things do in fact happen. I’m proud of the work my office has undertaken to go after the scammers that prey on Ohio families. My office will continue to provide support for local law enforcement in an ongoing effort to hold scammers accountable. We’re also committed to providing Ohioans with the information and education they need to avoid being victims in the first place.

By doing these things, we are making progress. Thank you, Mr. Chairman and members of the Committee. And I look forward to questions.

[The prepared statement of Mr. DeWine follows:]

PREPARED STATEMENT OF MIKE DEWINE, OHIO ATTORNEY GENERAL

Thank you Chairman Thune, Subcommittee Chairman Moran, and Ranking Member Blumenthal for holding this important hearing today to discuss how scams are affecting families in my home state of Ohio and families all across our country.

I have served now as Ohio Attorney General for just over six years. One of the things I am continually amazed by is both the number of scams that constituents report to my office and the increasing creativity of the scammers! As you all know, there have always been scam artists and cons. But, what is different today is that they now have the long arm of both the Internet and phones!

The Internet and social media have transformed the world we live in and the way we communicate. For example, grandparents who live miles apart from their grandkids, can now see them with the touch of a button on their mobile devices. Unfortunately, scammers also use these modern conveniences to commit fraud and satisfy their greed.

“Grandparent scams” are one of the most frequently reported—and most gut-wrenching—scams my office receives. My wife Fran and I are the parents of eight children—and now grandparents of 22 grandchildren. Like any grandparent, there is nothing we wouldn’t do for our grandkids. And that is exactly the mentality that the scammers prey upon.

The scam often begins with a phone call telling grandparents that one of their grandchildren has been in a car accident, caught with drugs, or put in jail. The caller pretends either to be the grandchild, an attorney, or a law enforcement officer and tells the grandparent to send money to have the charges dismissed, to cover court costs, or to allow the grandchild to return home.

There is always a sense of urgency with these scams. The grandparent is told to go to the store right away, to buy several gift cards, and to read the card numbers over the phone. Using this information, the scammer then drains the funds on the cards almost instantly.

As part of the scheme, grandparents often are instructed not to talk to other people (such as the grandchild’s parents) about the problem. Callers may even threaten to shoot or harm the grandchild if the grandparent refuses to pay.
And, if grandparents pay once, they likely will receive additional calls seeking more money, supposedly for attorney’s fees or other unexpected costs. Eventually, grandparents discover that their grandchild was not truly in trouble. But by then, it is too late. The average loss to an individual Ohioan because of this scam is $5,309. And that’s just based on the cases reported to my office. Because so many go unreported, that figure is likely much higher.

Another popular scam is the “romance scam!” In a typical romance scam, the con artist “meets” the victim online through a dating or social networking site. The scammer often claims to live in the United States, but says he or she is temporarily located overseas due to a military assignment, business trip, or personal vacation.

One common theme of this scam is that the victim never actually meets the scammer face-to-face. Instead, the scammer may spend months developing a relationship with the victim online. Eventually, he or she asks the victim to send money to help cover some type of cost, such as airfare to visit the victim, medical expenses, or fees associated with military leave. The scammer often asks the victim to send the money via wire transfer or prepaid money card. Not surprisingly, once the money is sent, it is nearly impossible to recover. The average loss to an individual Ohioan for this scam is $26,518! And again, that number is just based on cases reported to my office. It, too, is likely much higher.

As Attorney General, I have been committed to treating these scams as what they are—crimes. In 2011, I established an Economic Crimes Unit in my Consumer Protection Section. The unit includes seasoned prosecutors and investigators tasked with holding these fraudsters accountable and assisting local law enforcement and prosecutors in identifying, investigating, and prosecuting consumer fraud of a criminal nature. The unit consists of three attorneys and four investigators who are dedicated solely to criminal investigations.

To assist even more in the fight against scams, my office sought additional investigative power from the Ohio General Assembly in 2012. The result was new telecommunications fraud subpoena authority that our investigators and lawyers use every day to obtain financial and electronic evidence that furthers investigations and leads to arrests and prosecutions. This subpoena power is crucial in investigating scams that are exclusively Internet or phone-based.

Telephone and electronic communication are the major tools that scammers use to initiate contact with consumers. Unlike in the past, phone numbers are no longer a reliable indicator of where a call is coming from or who is making it. Voice over Internet Protocol (VoIP) phones allow callers to use area codes and phone numbers linked to a particular city or state, even though the person making the call is nowhere near there.

These services use a computer or smartphone to make calls through the Internet. Calls can be made using WiFi hot spots commonly found in airports, restaurants, coffee shops, and libraries. Criminals use the perceived legitimacy these phone numbers provide to help persuade unsuspecting victims into sending them money. We commonly see this tactic being used in IRS scams where the call appears to be originating from Washington, D.C. or Northern Virginia, but is instead coming from overseas.

Changes in how money is transferred have created additional challenges. Money transfer services, such as Western Union and Moneygram, were the traditional methods scammers used to get money. While those methods are still in use, we’ve learned that scammers now rarely receive the money directly. They tend to use “Money Mules,” who are people who’ve often been duped into thinking they’re “Secret Shoppers” or getting an advance for a babysitting job or think they have a job processing payroll to receive the money and send it on—often to someone overseas. These multiple steps are used to frustrate law enforcement and throw them off the trail. Also, people picking money up are required to provide very little, if any, formal identification, which further impedes our efforts to identify them.

Criminals have discovered another tool for moving money—prepaid gift cards and reloadable debit cards. Scam victims are instructed to purchase prepaid or reloadable cards, most recently iTunes cards. They then provide the unique identifying number from the back of the card to the scammer, and the money is transferred from the prepaid card or reload card to the scammer’s account almost immediately, leaving the victim holding nothing but a useless piece of plastic.

My office recently spoke with a victim who received a call telling her that her grandson had been in a car accident and that the judge would drop the charges if she paid $4,500 to an insurance company to cover the damage to a rented vehicle. The victim purchased prepaid cards, provided the card numbers to the scammer over the phone, and then was told to mail the cards themselves to an “insurance office” in Columbus, Ohio. My investigators found the address. As you would suspect, there was no insurance company.
Separate, but related, it’s probably no surprise to you that many scam victims are targeted solely because of their age. To address this issue, my office created the Elder Justice Initiative and assigned staff to work with law enforcement, prosecutors, Adult Protective Services, and communities to identify, investigate, and prosecute elder abuse cases. We also host forums in local communities to educate seniors about how to protect themselves from cons.

As much as we try to educate consumers about potential scams, these cons are good at what they do and continue to rip off the vulnerable. Though many times, our investigations lead to dead ends, sometimes our work pays off in getting these bad guys. In 2013, for example, my office indicted and convicted 18 defendants for a national telemarketing ring that stole more than $2 million from thousands of victims in 41 states over a five-year period. That group used dozens of VoIP phone numbers, seasoned telemarketers, false websites, elaborate lies, and multiple businesses in Ohio and Florida to prey on owners of vacant, nearly worthless land throughout the desert southwest.

Also in 2013, attorneys from our Special Prosecutions Section convicted John Donald Cody of running a charity scam that stole millions of dollars intended for Navy veterans. Cody, who had assumed the identity of a man named Bobby Thompson, was sentenced in an Ohio courtroom to 28 years in prison and ordered to pay more than $6.3 million in fines.

Just last month, my office partnered with local law enforcement and indicted a 66 year-old-woman for her role in an alleged romance scam. According to investigators, the suspect lied to people about needing money for various reasons, such as claiming she had a serious illness or that she was at risk of losing her home. The victims, who included the suspect’s family and friends, believed her. Although the suspect generally promised to pay people back promptly, investigators determined that she sent the funds overseas to a man she had been communicating with online. This person’s lies and deception cost her friends and family over $730,000!

This case comes on the heels of a 2014 investigation that my office initiated that led to a federally-convicted drug dealer pleading guilty to a running a romance scam that robbed over $1.1 million from unsuspecting victims across the country. The case began when my office received a complaint from an Ohio resident who had lost over $800,000 to a man she met online. My investigators tracked our victim’s money to accounts in Maryland. We then reached out to local law enforcement, shared what we had learned, and provided evidence linking a convicted drug dealer to the scheme.

The drug dealer was the ringleader to a group of scammers who used a number of false stories and promises to convince the victims to give money, including stories about investing in fake gold that required payments for shipping and storage, fictitious sick family members who needed money, fake hospital bills, and fake plane trips to visit the victims. To help conceal the scheme and by using false documents, the conspirators were able to convince the victims to mail checks to a corporation that one of the cons had created and controlled or to wire money into bank accounts held in the name of that corporation.

Because of that single lead, we were able to develop that case into a Federal investigation. It is that kind of state and Federal cooperation that has brought justice not only to our Ohio victim, but also to victims throughout the United States.

As we approach April, IRS scams become more prevalent. The IRS scams and tax preparer frauds pose special challenges for law enforcement. Because of Federal law, the Internal Revenue Service cannot and will not share tax or taxpayer information with our state criminal investigators. Let me tell you why that’s important.

Our investigators will receive a complaint about someone who is doing taxes and is alleged to be stealing part of the taxpayer’s refund by personally diverting the money. This single taxpayer can get his or her own records and provide them to us, but our investigators have no way of knowing how much larger the crime may be or how many more people may be being victimized because the IRS can’t tell us anything at all. State subpoenas won’t work, so our investigation ends up at a dead end.

The individual loss for this type of scam is generally less than $2,500.00. But, because we can’t get access to information about other potential victims, that’s where the case stops.

Whenever we receive an allegation of tax preparer fraud, IRS scam calls, or refund theft, we tell the consumer to contact the Treasury Inspector General for Tax Administration (TIGTA). Very few of these cases are ever likely to meet the dollar threshold required to get the attention of an IRS inspector, let alone a U.S. Attorney. Giving state and local law enforcement the ability to obtain the information needed to effectively investigate and prosecute tax preparer fraud, IRS scams,
refund theft wouldn’t just protect taxpayers, it would conserve valuable Federal resources and help ensure the integrity of our tax collection program.

There is strength in numbers. When multiple agencies put their resources, intelligence, and ingenuity together, great things can happen.

Ohio is a home rule state, with 88 counties and 88 county sheriffs and prosecutors acting independently from the other 87. That local control ensures that those elected officials are accountable to the people in their communities. It also ensures that these sheriffs and prosecutors know what’s happening in their counties.

But, there are also challenges. A law enforcement officer in Jackson County, for example, may know about the three people who were ripped off in that county, but may not know about the three people who were victimized in Greene County, or the two people who were victimized in Clark County, or the person who was conned out of her life savings in Ashtabula County. Imagine how much bigger that problem gets when you start talking about victims in multiple states and victims who are hundreds or even thousands of miles away.

One of the reasons our Economic Crimes Unit has been successful is that we’re able to see patterns of conduct occurring across multiple counties, make connections with law enforcement and victims, and show the true scope of a criminal enterprise. We need to apply that same logic to scams and economic crime nationwide. To be successful, we need to break down barriers to communication, sharing information, and resources and work together to combat crime on the national and international level.

We’ve seen that model work in Project JOLT, where the U.S. Department of Homeland Security has partnered with the Jamaican Constabulary Force, industry, and other law enforcement agencies to take down Jamaican lottery scammers—a number of whom have recently been extradited to the United States to face Federal charges. Now is the time to apply those lessons to others scams and crimes.

I am very proud of the work my office has undertaken to go after the scammers that prey on Ohio families. My office will continue to provide support for local law enforcement in an ongoing effort to hold scammers accountable. We’re also committed to providing Ohioans with the information and education they need to avoid being victims in the first place. By doing these things, we are making a difference.

Thank you, again, for the opportunity to testify here today. I’m happy to answer any questions.

The CHAIRMAN. Thank you, Attorney General.

Mr. Abagnale.

STATEMENT OF FRANK ABAGNALE, AUTHOR AND CONSULTANT, ABAGNALE & ASSOCIATES

Mr. ABAGNALE. Thank you, Chairman Moran and Ranking Member Blumenthal and members of the Committee. I am honored to be invited to testify before you today on the seriousness of identity theft and financial fraud against the elderly and all American citizens and the need for education to prevent individuals from falling victim to these multiple scams.

I’m Frank Abagnale, subject of the book and movie “Catch Me If You Can.” I have a unique perspective, having committed fraud as a teenager some 50 years ago, and having spent the last 41 years of my life teaching at the FBI Academy and the field offices of the Federal Bureau of Investigation.

Over the past 4 decades, I’ve conducted over 3,000 lectures and written four books on these subjects. During this time, I’ve worked to try to prevent fraud, forgery, cyber crimes, embezzlement, identity theft, and other scams perpetrated against consumers and small businesses.

Serious issues we face are fraud and scams which are perpetrated against American citizens of all ages. They can be perpetrated by family members, financial advisers, home health care providers, friends, scam artists, and others.
Let me share with you some statistics that speak volumes as to why we need initiatives to help prevent these frauds against consumers.

A new survey by Javelin Strategy & Research shows a 16 percent growth in fraud incidences in 2016. Fraud affected over 6 percent of U.S. consumers, the highest on record. The Consumer Sentinel Network, which collects consumer complaints from the Federal Trade Commission, state law enforcement agencies, and other Federal agencies received over 3 million complaints in 2016. Almost 1.3 million of those complaints were fraud-related. Consumers reported paying over $744 million in those fraud complaints.

The FBI’s Internet Crime Complaint Center issues an annual report based on reported complaints of Internet crime. The 2015 report—and that’s the latest available—shows that the center received nearly 270,000 online crime complaints in 2014, with a loss of about $800 million. State-by-state complaint data shows the largest losses are from individuals age 50 plus.

These are probably low estimates because many times consumers are too embarrassed to admit that they have been defrauded, and, therefore, it goes unreported. Their families might not even be told. Identity theft, investment fraud, and scams rob millions of Americans of their hard-earned money every year.

To help combat this threat, for the last 3 years, I’ve joined forces with AARP’s Fraud Watch Network as their Ambassador. The goal of the Fraud Watch Network is to arm Americans with tools they need to spot and avoid fraud and scams so they can protect themselves and their families. Last year, through my relationship with the Fraud Watch Network, we reached more than 43 million people through state office sponsored events, social media, e-mail alerts, and online advertising. We held more than 1,200 events on the topic of fraud in 2016 alone. In 2017, I will be appearing in more than one dozen cities across America to help educate people about current scams, their risk, and most important of all, how to protect themselves and their families from being victimized.

What is truly amazing to someone like me is that what I did 50 years ago as a teenager is 4,000 times easier to do today due to technology. Unfortunately, technology breeds crime; it always has and always will. At the same time, there is no technology, nor will there ever be any technology, that can prevent social engineering. Socially-engineered crimes can only be prevented through education. There will always be individuals who will use technology in a negative, self-serving way.

Throughout my career, I have always believed that education is the best prevention. If you educate and explain to people their risks, in most cases, they are smart enough to take that information and reduce their risk. I believe education is the only approach to help eliminate consumer fraud. Education is not only important for our seniors, but it also helps bring awareness to all citizens so they can recognize the signs of fraud and how to protect themselves.

I have always believed that the government should take the lead in education to combat these horrendous crimes. Consumers are hungry for information but do not know about legitimate resources where they can turn for help. Over the last 2 years, I have given
my time to film public service announcements for both U.S. Department of Justice and numerous state attorney generals to help the public awareness.

As the Committee is aware, there is very little prosecution for these crimes and almost no restitution. Once you lose your money, your chance of getting it back is extremely slim. Unfortunately, many of these criminals are operating from other countries, where we do not have legal authority to make an arrest and follow through with prosecution. I believe that law enforcement and the Federal Trade Commission need to take these crimes against consumers more seriously and push for arrest and convictions of criminals making victims of innocent people when there is enforcement power to do so.

Thank you for the opportunity.

[The prepared statement of Mr. Abagnale follows:]

PREPARED STATEMENT OF FRANK ABAGNALE, AUTHOR AND CONSULTANT, ABAGNALE & ASSOCIATES

Chairman Thune and members of the Committee, I am honored to be invited to testify before you today on the seriousness of identity theft and financial fraud against the elderly and all American citizens and the need for education to prevent individuals from falling victim to these multiple scams.

I am Frank Abagnale, subject of the book and movie “Catch Me If You Can.” I have a unique perspective, having committed fraud as a teenager some 50 years ago, and having spent the last 41 years of my life teaching at the FBI Academy and field offices of the FBI. Over the past four decades, I have conducted over 3,000 lectures and written four books on these subjects. During this time, I have worked to try to prevent fraud, forgery, cybercrimes, embezzlement, identity theft and other scams perpetrated against consumers and small businesses.

Serious issues we face are fraud and scams which are perpetrated against American citizens of all ages. These can be perpetrated by family members, financial advisers, home healthcare providers, friends, scam artists, and others. Let me share with you some statistics that speak volumes as to why we need initiatives to help prevent these frauds against consumers.

A new survey by Javelin Strategy & Research shows a 16 percent growth in fraud incidence in 2016. Fraud effected over 6 percent of U.S. consumers—the highest on record.

The Consumer Sentinel Network, which collects consumer complaints from the Federal Trade Commission, state law enforcement agencies and other Federal agencies, received over 3 million complaints in 2016.

- Almost 1.3 million of those complaints were fraud-related.
- Consumers reported paying over $744 million in those fraud complaints.
- The FBI's Internet Crime Complaint Center (IC3) issues an annual report based on reported complaints of Internet crime. The 2015 report (the latest available) shows that—
  - The center received nearly 270,000 online crime complaints in 2014 with a loss of about $800 million.
  - State-by-state complaint data shows the largest losses are from individuals age 50+.

These are probably low estimates because many times consumers are too embarrassed to admit that they have been defrauded, and therefore it goes unreported. Their families may not even be told. Identity theft, investment fraud and scams rob millions of Americans of their hard-earned money every year. To help combat this threat, for the last three years I have joined forces with AARP’s Fraud Watch Network as their ambassador. The goal of the Fraud Watch Network is to arm Americans with the tools they need to spot and avoid fraud and scams so they can protect themselves and their families. Last year through my relationship with the Fraud Watch Network we reached more than 43 million people through state office sponsored events, social media, e-mail alerts and online advertising. We held more than 1,200 events on the topic of fraud in 2016 alone. In 2017, I will be appearing in more than one dozen cities across America to help educate people about current
scams, their risks and most important of all, how to protect themselves and their families from being victimized.

What is truly amazing to someone like me is that what I did 50 years ago, as a teenager is 4,000 times easier to do today due to technology. Unfortunately, technology breeds crime, always has and always will. At the same time, there is no technology, nor will there ever be any technology that can prevent social engineering. Socially engineered crimes can only be prevented through education. There will always be individuals who will use technology in a negative, self-serving way.

Throughout my career, I have always believed that education is the best prevention. If you educate and explain to people their risks, in most cases they are smart enough to take that information and reduce their risks. I believe education is the only approach to help eliminate consumer fraud. Education is not only important for our seniors, but it also helps bring awareness to all citizens so they can recognize the signs of fraud and know how to protect themselves.

I have always believed that the government should take the lead in education to combat these horrendous crimes. Consumers are hungry for information but do not know about legitimate resources where they can turn for help. Over the last two years, I’ve given my time to film public service announcements for both the U.S. Department of Justice and numerous state attorneys general to help with public awareness.

As the Committee is aware, there is very little prosecution for these crimes and almost no restitution. Once you lose your money, your chance of getting it back is extremely slim. Unfortunately, many of these criminals are operating from other countries where we do not have legal authority to make an arrest and follow through with prosecution. I believe that law enforcement and the Federal Trade Commission need to take these crimes against consumers more seriously and push for arrests and convictions of criminals making victims of innocent people when there is enforcement power to do so.

Thank you.

The CHAIRMAN. Mr. Schwanke.

STATEMENT OF MIKE SCHWANKE, REPORTER, KWCH-12 EYEWITNESS NEWS

Mr. SCHWANKE. Chairman Moran, Ranking Member Blumenthal, committee members, thank you for this incredible opportunity to talk about an issue that affects all Americans. In my 17 years as a journalist and investigative reporter, I have focused much of my time helping victims of scams, but also educating the public so they don’t fall victim.

I am honored to be invited here today by Senator Moran. The Senator and I go back almost 2 decades now to my days as a bureau reporter in Dodge City. Then Congressman Moran would often stop by my office and talk about the issues affecting Kansans. But the issue we address today does not stop at a state line. Scams and those who perpetrate them stop at nothing. No person is immune, not even in our darkest times, because scammers wait to take advantage.

This month, Kansas experienced our largest wildfire event in the state’s history. Homes and livestock were lost. And while Kansans and surrounding Midwest states all came together to help each other, shockingly, there were those who only saw an opportunity to steal. Instead of solely focusing on protecting lives and property, Reno County Sheriff Randy Henderson instead had to spend time warning his residents about a scam. During a time of disaster, victims of the fire were receiving calls from someone offering free Federal grants. All they had to do was send in an application fee. That scam was underway before most victims were even allowed back into their homes to survey the damage.
Scammers don't see tragedy, they see opportunity, like when Wichita Police Officer Brian Arteburn was critically injured last month. He was run over by a fleeing suspect, but within days, we had to warn our viewers of a telephone scam collecting money in his name.

Our seniors are most at risk because they often have the most to lose. They feel there is no one out there to protect them. Much of my time is spent in churches and senior organizations trying to educate.

Those in our most trusting generation rarely go a single day without someone trying to trick them, scam them, and ultimately steal the money they have worked their lifetime to earn. I know because we talk to them. My producer now receives about a dozen calls from victims every week. Last week, that number grew to 20. I personally have told the stories who have wired away their entire life savings, and that money usually goes overseas, never to be seen again. That scammer starts again usually with another unsuspecting American.

I could be here for hours sharing stories of victims, like the Wichita woman in her seventies we interviewed who was taking care of her elderly mother. She was targeted by a scammer looking to take advantage of her willingness to help others. She had about $25,000 left to care for her mother, and lost every cent.

There was another couple who fell for what is commonly referred to as the grandparents scam, which you've heard about today. Thinking he was helping his granddaughter in distress, the 88-year-old walked into two Wichita grocery stores and purchased $13,000 in iTune cards. The money was gone. The man's wife told me she had just seen us do a story on that very scam, but the scammers were so convincing and she was so scared, she fell for it anyway. That same scam has also been used on our military families in Kansas.

What's more concerning are those we don't know about, those who are too embarrassed or afraid they'll lose their financial freedom if they share their stories. I often get calls from victims who want to share their story to protect others, but ask that I shield their identity.

We often hear about seniors falling victim, but one of our investigative stories found that Millennials may be even more likely to fall for scams. The Better Business Bureau now backs that up, releasing a study this month that found consumers 18 to 24 years old are most likely to lose money in a scam.

Alex Cook is one of them. The 19-year-old called me after she fell victim to a scam on Care.com. The teen, who was working three jobs at the time to pay the bills, lost $2,600, and it set her back 6 months.

Even our county government and businesses have lost hundreds of thousands of dollars to scams. The estimated loss to the American economy is in the billions, and some estimates show as many as 1 in 10 Americans will lose money to a phone scam every year.

Top scams reported by the BBB last year include the tax collection, debt collection, lottery, and online purchase scams. Our District Attorney's Consumer Protection Division fields now about
2,000 calls a year, so many the office had to develop a new system to handle the calls because they were overwhelmed.

The Wichita Police Department has four detectives in its Financial Crimes Division, each one now has 60 active cases at any given time. In 2015, there were 3,800 cases; last year, 7,000. Rarely can local law enforcement or prosecutors do anything about the cases because they often take them out of their jurisdiction.

In closing, what we have found in our reporting is many times scammers use fear and intimidation to steal from victims. Law enforcement and prosecutors can do little to stop it. The best weapon we have right now is education, but it has to be consistent because tomorrow there will be a new scam, new tactics, and Americans will lose more money.

Again, I thank you for the invitation to be here today and look forward to any questions you may have.

[The prepared statement of Mr. Schwanke follows:]

PREPARED STATEMENT OF MICHAEL SCHWANKE, REPORTER, KWCH–12 EYEWITNESS NEWS

Chairman Moran, Ranking Member Blumenthal, and Committee members—I thank you for this incredible opportunity to talk about an issue that affects all Americans.

My name is Michael Schwanke with KWCH TV in Wichita, Kansas. In my 17 years as a journalist and investigative reporter I have focused much of time on helping victims of scams and educating the public so they don't fall victim. I'm honored to be invited here today by Senator Moran. The Senator and I go back almost two decades to my days as a bureau reporter in Dodge City. Then Congressman Moran would routinely stop by my office and talk about the issues affecting Kansans.

But, the issue we are addressing today doesn't stop at a state line. Scams and those who perpetrate them, stop at nothing. No person is immune, and even in our darkest times scammers wait to take advantage.

This month Kansas experienced the largest wildfire event in the state’s history. Homes and livestock were lost. While Kansans and surrounding Midwest states came together to help each other, shockingly there were those who saw an opportunity to steal. Instead of solely focusing on protecting lives and property, Reno County Sheriff Randy Henderson had to warn his residents about a scam. During a time of disaster, victims of the fire were receiving calls from someone offering free Federal grants. All they had to do was send in an application fee. The scam was underway before some victims of the fire were even allowed back in to survey what they'd lost.

Scammers don't see tragedy, they see opportunity like when Wichita Police officer Brian Arteburn was critically injured last month. He was run over by a fleeing suspect. Within days we had to warn viewers of telephone scam collecting money in his name.

Our seniors are most at risk, because they often have the most to lose. They feel there is no one to protect them. Much of my time is spent in churches or senior organizations trying to educate.

Those in our most trusting generation rarely go a single day without someone trying to trick them, scam them and ultimately steal the money they've worked a lifetime to earn. I know, because we talk them. My producer now receives up to a dozen calls from victims every week. Last week that number grew to more than 20.

I personally have told the stories of those who have wired away their entire life savings. The money usually goes overseas never to be seen again. The scammer then starts again, with another unsuspecting American.

I could be here for hours sharing stories of victims—like the Wichita woman in her 70s we interviewed who was taking care of her elderly mother. She was targeted by a scammer who took advantage of her willingness to help others. She had about $25,000 left to care for her mother and lost it all.

There was another couple who fell for what's commonly referred to as the grandparent scam. Thinking he was helping his granddaughter in distress, the 88-year-old walked into two Wichita grocery stores and purchased $13,000 in I-Tune cards. The money was gone. The man's wife told me she had just seen me do a story on
this very scam. The scammers were so convincing and she was so scared, she fell for it anyway. The same scam has been used on military families in Kansas.

What’s more concerning are those we don’t know about—those who are embarrassed and afraid they will lose their financial freedom if they share their stories. I often get calls from victims who want to share their story to protect others, but ask that I shield their identity. We often hear about seniors falling victim, but even one of our investigative stories found that millennials may be even more likely to fall for scams. The Better Business Bureau backs that up, releasing a study this month that found consumers 18–24 years old are most likely to lose money in a scam.

Alex Cook is one of them. The 19-year-old called me after she fell victim to a scam on Care.com. The teen, who was working three jobs at the time, lost $2,600. It set her back six months.

Even our county government and area businesses have lost hundreds of thousands to scams.

The estimated loss to the American economy is in the billions. Some estimates show as many as one in 10 Americans will lose money to a phone scam every year. Just last year the Better Business Bureau worked with more than 5,000 victims who lost more than $42 million.

The top scams reported to the BBB last year include tax collection, debt collection, lottery and online purchase scams.

And what happens when they report it? Usually nothing.

Our District Attorney’s Consumer Protection Division fields about 2,000 calls a year. So many the office had to develop a new system to handle the calls because they were overwhelmed. There is one attorney in the consumer protection division.

The Wichita Police Department has four detectives in its financial crimes division. Each one has up to 60 active cases at any given time. In 2015 they were 3,800 cases. Last year 7,000. Rarely can local law enforcement or prosecutors do anything because the cases take them out of their jurisdiction or they simply don’t have the resources. By the time police are able to obtain proper warrants or subpoenas, the scammers have moved on.

In closing, what we have found in our reporting is many times scammers use fear and intimidation to steal from victims. Law enforcement and prosecutors can do little to stop it. The best weapon we have at this point is education, but it has to be consistent. Tomorrow there will be a new scam, new tactics and Americans will lose money. Again, I thank you for the invitation to be here today and look forward to any questions you may have.

The CHAIRMAN. Thank you very much. Let me start with Chairwoman Ohlhausen. Is there a reliable financial macro cost to scams in the United States? Do we know from the side of the personal aspects of this, what does it cost the economy?
Commissioner Ohlhausen. Well, based on the redress that the FTC has been able to get for consumers, even just last year, it cost billions and billions of dollars. So we get redress for consumers, and last year we were able to get more than a billion dollars, well, several billion dollars, a lot of that was driven by the VW settlement, which was about $10 billion or $11 billion. So it is billions and billions of dollars.

The Chairman. Mr. Schwanke, in your investigations and your attempts to help Kansans, have you discovered any place that it makes most sense for a victim to go with his or her problem? Who is best at providing relief and satisfaction?

Mr. Schwanke. I think that's a lot of their frustration. I think once they've been a victim of a scam, they often turn to the Better Business Bureau or us to warn others, and oftentimes they understand that that is their only option at that point, is to stop it from happening to anyone else. Calling law enforcement often goes nowhere just because they can't do anything.

The Chairman. You indicated something that was discouraging to me because one of the conversations we've had already just in this hearing is the value of information, but you indicated that in a particular instance, the victim had seen the similar identical fraud being talked about on your program, but still felt necessary to respond to the cries of a grandchild. Do you have evidence that this consumer awareness actually makes a difference? Do you have instances in which you've been told, "I saw your program. It warned me, and the same thing about happened to me, but I knew not to fall for it"?

Mr. Schwanke. That's one example. Oftentimes we do hear from victims who say, "I knew better," and when they see these stories of victims, they sit back in their home and think, "How in the world could I ever fall for something like that?" In that case, she saw our story, and she explained it as tunnel vision. And I think that's what these scammers depend on. When I talk to these senior groups and I lay out these scams, and even the crowd will say, "Well, I would never fall for that," but I used her as an example of once she thought that her granddaughter was in trouble, she said, "It was almost like I had blinkers on, and that's the only thing I could see at that point."

So in that story, that is really what she tried to get across to viewers, is you really have to stop and think because you are not going to be thinking clearly when someone calls for a grandparents scam or someone calls claiming to be with the IRS saying that they're going to haul you off to jail if you don't pay your taxes. Once you hear that, your mind shuts off oftentimes. That's what we try to get across in our education.

The Chairman. General, you've been involved in public service announcements. Is there evidence that they're useful, successful, and prevent additional fraud?

Mr. DeWine. We do get calls, Mr. Chairman, from people, and sometimes I'll actually see people who say, "I saw you on TV talking about the grandparents scam," or, "I saw you on TV talking about the IRS scam." So while we are successful in some prosecutions, the ones that are over the Internet, the ones that are long distance, are very, very difficult for all of the reasons that have al-
already been stated. And, frankly, we think that our prime job in this case is to really warn people, trying to warn them about this.

So, yes, we have some results, but it’s the same, we’ve all, I think, had the same experience. You know, many times people say, “I never would have thought I would fall for this, but I did,” and what I think the public sometimes thinks is, “Well, I wouldn’t do that,” or they think these are people who aren’t very smart. That’s not true. These are smart people. These are average just regular people who you find in Ohio, and because some button has been pushed, whether it is the compassion for your grandchild, or in the case of the IRS scam, where they call you up and threaten you, it’s just total fear, that emotion overrides.

The CHAIRMAN. Mr. Abagnale, regarding the perpetrator of a fraud, what is it about them that allows them to be able to get that, elicit that, response from somebody who is apparently smart and has seen information about the potential scam and still falls for it? What’s the way to capture somebody?

Mr. ABAGNALE. Well, first of all, thank God that the majority of Americans are honest, and because they’re honest, they don’t think in a deceptive way. So when the phone rings and the caller ID says it’s the Internal Revenue Service or U.S. Government or their local police department, they believe that to be true. They’re not aware that the caller ID is easily manipulated. So people believe at the start that the call is legitimate. And then the person on the other end of that call can be very, very persuasive in getting people to give them information or to get money from them with some of these scams that we’ve heard about here today that are very common.

Now, we’ve said so much about the IRS scam over the last few years and have reached so many American citizens about it that the criminal is now changing gears a little bit realizing that a lot of people know that when you get a call from the IRS demanding money, that the IRS usually doesn’t make phone calls, that they would write you a letter.

So the scammers in the last year have started writing letters on the IRS letterhead, postage paid by the Federal Government over on the right-hand corner of the envelope, and mailing out letters supposedly from the IRS with a reference number up in the top right corner, and simply saying to call this 800 number to speak with Agent So-and-so. And, of course, someone answers, “Internal Revenue,” they connect you to that person, who is not really that person.

So, as you can see, they’re able to understand how it works. When it gets a little tight or they realize people are catching on, they switch gears a little bit and go to something a little more sophisticated.

Again, through my entire career, I believe that if you explain to people these scams, you tell them how they work, that’s the best way to prevent those scams from occurring. When I go out with AARP Fraud Watch Network, I spend my afternoon on the phone speaking to about 15,000 people who call in to the AARP’s office, state office, and get on the line, and they hear about all these scams and get to ask me questions about things that have happened to them and how to understand how some of these work. I
find that it’s a very powerful tool of reaching people and getting that information.

It’s interesting to me that back in the 1970s, before there was ever a book about me, I did some public service ads for the Department of Justice that were given to police departments across the country. Those ads ran for years on television. They were 30-second ads. The police department was able to put their logo at the end of it, sponsored from that police department. In the 1980s, only a book had been written about me, and those people didn’t know who I was, but I actually did millions of bank statement stuffers for banks that went out to people in their bank statement, and it had tips about protecting their checkbook, protecting their credit cards.

Today, there is very little of that. We very rarely see public service ads on TV. We very rarely see that reaching out to explain to people what is going on. I think we need to get back to that. It’s very important, and it’s the only way to really fight crime, is through education. And I think that’s the way that I try to approach it in the 40 years I’ve been doing this.

I would remind you, the Committee, of one thing. I always teach FBI agents to follow the money, and have for 4 decades. So what we find is that most of these crimes that are committed by people living in Russia, India, China, that are making these calls in their pajamas or on their laptop from their kitchen, are stealing money from the American consumer. It is leaving our economy, but it will come back, it always comes back, because it will tend to boomerang and return to our country, but in the form of drug trafficking, human trafficking, child pornography, and much more hideous crimes.

So it is very important that we try to prevent that money getting in the wrong hands of people who are going to do a lot worse—commit a lot worse crimes with that money.

The CHAIRMAN. Thank you.

Senator Blumenthal.

Senator BLUMENTHAL. Thanks, Mr. Chairman.

Let me ask you, Chairwoman Ohlhausen, as you know about mobile cramming, it is the unscrupulous practice by wireless carriers of allowing third parties to add charges onto their monthly bills without authorization by the consumer. And in many, many cases, the consumer receives nothing for those charges, or receives something they didn’t want, didn’t know they were going to get. And this practice has been a problem for 2 decades or more, and it’s really not much more or less than outright theft.

In 2013, the FTC brought numerous enforcement actions then and since against wireless carriers, including T-Mobile and AT&T, for those corrupt practices, which I welcome and I’ve lauded and thank you for doing because the settlements have reached as high as $105 million and $90 million in refunds, fines, and penalties. The wireless industries and companies across the board should protect their consumers from these kinds of abuses.

I’m hoping that you will commit that the FTC will continue to pursue these cases by holding both individuals and companies that may have aided and abetted them accountable no matter how insulated or big they may be.
Commissioner OHLHAUSEN. Ranking Member Blumenthal, thank you for mentioning those cases. I have been personally very supportive of the FTC’s cramming cases. I’m concerned about our ability to continue to act in that space given the Ninth Circuit’s decision on the common carrier exemption.

Senator BLUMENTHAL. But given the legal ability to do so, will you commit to holding the aiders and abettors accountable to the maximum degree you can?

Commissioner OHLHAUSEN. To the extent we are capable of doing that under our current authority, I would certainly commit to that. As you may recall, we’ve been able to reach certain actors, like particularly in the Western Union case, under our unfairness authority.

Senator BLUMENTHAL. Commissioner McSweeny, do you agree?

Ms. MCSWEENY. Yes, I strongly agree. I think that Congress has from time to time seen fit to give us assisting and facilitating authority, for example, in the Telemarketing Sales Rule Act, and I think that kind of authority is very, very helpful in making sure that we can not just play the game, as you alluded to, of “Whack-A-Mole,” of going after fraudsters, but also making sure that we’re holding people accountable if they know that they are facilitating fraud and processing those payments.

Cases like the Western Union case are very, very important, because a huge amount of the money that was transferred out in the kinds of scams you’ve just been hearing about out of our country to other countries was transferred through that system. And so having that entity have more accountability and, in fact, acknowledge that they are doing a much better job policing their own platforms is very, very important to protecting consumers in the first place. So I think that’s an important area, not just in cramming, but across all industries.

Senator BLUMENTHAL. Thank you. A lot of consumers probably have no idea that new car dealers are prohibited from selling vehicles with open recalls, but used car dealers are free to do so, even though the defects can be deadly, and the recalls can be very, very important. In fact, used car dealers can advertise cars with unrepaired safety recalls saying they are, “safe,” or have passed “rigorous inspection”, even if they have defective Takata airbags that can explode and kill them or maim them, and other potentially deadly defects.

This disclosure issue is extraordinarily important. And as long as I am a member of this committee, I am going to continue working to try to close that gap in the law. I disagree with the FTC’s proposed final orders against GM, Jim Koons, and Lithium Motors for their deceptive advertising actions. If you could tell me just very simply yes or no, in your opinion, to the two Commissioners, the Chairwoman and Commissioner McSweeny, in your opinion, is a car with an open unrepaired recall a safe car?

Commissioner OHLHAUSEN. If it was advertised as safe, I would have a concern about that.

Senator BLUMENTHAL. If it’s advertised as safe?

Commissioner OHLHAUSEN. Right. If there is a claim made that this car is safe, then I would have a concern if it had an open recall without a disclosure about that.
Senator Blumenthal. What about if it’s just—if it just has a deadly defect? Would you call it safe without any advertisement?

Commissioner Ohlhausen. I’m not sure that this—that’s an FTC issue. I mean, I may not personally call it safe, but under the FTC Act, we have to look at the claims that are made.

Senator Blumenthal. Commissioner McSweeny?

Ms. McSweeny. I strongly share your concerns about the sale of used vehicles with open safety recalls. This has resulted in documented tragedy. We struggled, I think, with the scope of the FTC authority in those cases, and I strongly support your efforts to provide a better solution to consumers to this problem.

Senator Blumenthal. Thank you both. And thank you to all the members of our panel. I apologize in advance. I probably will have to leave early because we have an ongoing confirmation hearing in the Judiciary Committee concerning Judge Gorsuch to the United States Supreme Court, so I will probably have to go back to that.

But I want to thank again the Chairman of this Subcommittee, Senator Moran. And I also want to thank the Chairman of our Committee, Senator Thune, who has just arrived. And he has enabled us to go forward with it. It’s very important. And I hope we can continue this work. Thank you.

The Chairman. Senator Blumenthal, thank you very much. We attempted to change the hearing. We would have lost our witnesses, and Senator Blumenthal was agreeable to us proceeding despite his demanding schedule, as a Member of the Senate Judiciary Committee now considering a nominee to the U.S. Supreme Court. I think you made that point, didn’t you?

We are honored to have the Full Committee Chairman join us today, and I now recognize Chairman Thune.

STATEMENT OF HON. JOHN THUNE, U.S. SENATOR FROM SOUTH DAKOTA

Senator Thune. Well, thank you, Mr. Chairman, and thank you, Senator Blumenthal, for having the hearing. I want to thank our panel, too. This is an important issue. It affects American consumers. And clearly consumers need protection from those who would seek to defraud them through scams. I think we can all agree the best use of the FTC’s resources is to pursue conduct and practices that cost Americans billions of dollars without any benefits.

I just wanted to highlight one example of how this sort of plays out in the real world. Last summer, I participated in a telephone town hall that was sponsored by AARP where the bulk of the calls focused on these kinds of scams.

And I, for instance, heard from a constituent named Louella from the town of Salem, South Dakota, who had twice been the victim of the so-called grandparents scam. In her case, not only did she receive a call from someone posing as a grandchild who claimed to be in jail and in desperate need of bail money, but when she wavered, she got a follow-up call from someone claiming to be a police officer verifying that her grandchild would remain in custody until the bill was paid.

And in her case, fortunately, she talked to her son who assured her that her grandkids were home safe. But it’s still not hard to
imagine the grandparent hoping to save their grandkids from em-barrassment and legal peril by wiring money to such a scammer.

And so I appreciate the subject of this hearing. It is an important issue that does affect people all across our country and across our states, and very grateful, a great panel.

And, Senator DeWine, so nice to have you back. Welcome. It’s good to see a former colleague. And so thank you for being here. I just want to ask one quick question because I know my colleague from Oklahoma I think has been waiting patiently, as have some of our colleagues on the other side.

But, Mr. Abagnale, we’ve talked about several different types of scams that hurt American consumers. I guess the question I would have is, is there a particular scam that worries you the most that you would like to highlight in terms of the things that are out there?

Mr. A BAGNALE. Obviously, I am very concerned about the breaches we read about literally every day without exaggeration, some reported, some not reported. We’ve had over a billion people have their identity stolen already. When I first started writing about identity theft, 750,000 victims filed a police report. Today, there’s a victim every 2 seconds in the United States.

I’m a true believer that most all breaches occur because somebody in that company did something they weren’t supposed to do or somebody in that company failed to do something they were supposed to do, and that most of those breaches can be easily prevented. Again, there is social engineering that occurs, et cetera.

I had a call at my home just a couple of days ago from the CFO of a large technology company on the West Coast, 4,000 employees. He said that someone in bookkeeping had received an e-mail from the CEO saying he needed all the W-2 files on all the 4,000 employees e-mailed up to him. The only reason they found out about it a couple of days later, someone from bookkeeping called up to the CEO or sent an e-mail to say, “I hope you got all the material you requested,” and he said, “I didn’t request that.” Four thousand employees’ information is now on the street.

I’m a big believer you verify. So if I was in that accounting department, that would be an unusual request. I would have got up, walked up to the CEO’s office, and said, “Did you in fact send me this e-mail?” or if they’re out of state, to get in contact with them over the telephone and make sure I spoke to them.

So all of these scams that we hear about, whether it be the grandparents scam, the sweepstakes scam, the IRS scam, is really that I tell people all the time, you just simply need to stop and verify. So if I call and I say I’m from the police department, it comes up on my caller ID I’m from the police department, I hang up the phone, I pick up the phone book, I don’t take the number they gave me, I look up the police department’s number in the phone book, I call the police department and say, “Do you in fact have my grandson in custody at the police department?” or, “Did you make a call to me for his bail?”

And that’s the main message, that you prevent most of these crimes, just simply stop and verify, whether it’s a large corporation, a small business, or an individual, you teach people that you have to check things out.
We had 56 million phishing scams in 2016, 5,000 every single day of the week, 7 days a week, each day. People need to learn that just because an e-mail comes in, the e-mail looks legitimate, if it is specifying information or requesting information that could be devastating to the clients, to their customers, to their employees, they need to verify that that e-mail is correct. Those are the things that worry me the most, that these breaches happen every single day, and more and more information is given away every single day.

Senator Thune. Thank you. And thank you, Mr. Chairman, for your leadership on this issue and on our committee. And again thanks to the panel. My time is expired. And I’m sure you hear this all the time, but you really are better looking than Leo DiCaprio. [Laughter.]

Senator Thune. Thank you.

The Chairman. The Senator from Oklahoma, Senator Inhofe.

STATEMENT OF HON. JIM INHOFE,
U.S. SENATOR FROM OKLAHOMA

Senator Inhofe. Thank you, Mr. Chairman.

All right, Mr. Abagnale, how close to reality was the movie?

Mr. Abagnale. I didn’t have a lot to do with the movie. I obviously would have preferred not to have a movie made about my life. As you know, I raised my three sons in Oklahoma to keep them away from just that, even though I officed here in D.C., and commuted back and forth. I saw you on the plane all the time with your lovely wife. However, I thought that he did a very good job of telling the story.

As he said many times, he loved the redemption side of the story. He had owned the rights for more than 20 years. He bought the rights back when he was making the movie with the shark, Jaws, and when Barbara Walters asked him why he waited so long to make the movie, he said, “I waited to see what Frank Abagnale did with his life before I immortalized him on film.” And so in the end, I think he was very much into the redemption side of the story, and I was probably very fortunate that it was he who told the story.

Senator Inhofe. Yes. Well, thank you. You know, back in your scamming days, if there is any truth to the story, you were always one step ahead. You knew where to go if the old technology wasn’t used, working, you would try something else. As you apply that background to what’s out there now, you mentioned in your opening statement that there are things that shift around for a while, the technology we’ll be working on, maybe the grandparents. What do you see in the future now as a prospect for scamming in the future that is not there now?

Mr. Abagnale. Well, you know, up until this—up until present day, cyber crime, for example, is all about money and getting information. I’m very concerned that cyber crime in the next few years is going to turn very black. So we have the ability now to shut someone’s pacemaker off, but we have to be within 35 feet of that individual to shut that pacemaker off or speed it up. We have the ability to get within 35 feet of an automobile, shut off the car, turn on the airbags, lock the person in the vehicle. Again, we need to
be within 35 feet. I believe that within the next 5 years you’ll be able to do that from 5,000 miles away.

So I am very concerned about our infrastructure. I’m very concerned about our electrical grid. These are the things that I think eventually cyber crime will come to be more of a terrorist tool and more of as a tool to eliminate individuals, and that’s when it will get very, very scary.

Senator INHOFE. Yes, and that is scary. It happens that the one sitting to your right is an old friend of mine from the House, and the two of us know more about grandkids than anybody else probably in this room, and he forgot to introduce his wife. So I’ll introduce her.

Fran, hold your hand up.

All right. Mr. Schwanke, I was fascinated, first of all, that was the worst wildfire in the history of Oklahoma and Kansas. And I got in my little plane last week and went up to Woodward. And then yesterday I was in Buffalo, Oklahoma, and we had over 300 farmers and ranchers, half of them were from Kansas. And not one time in those meetings did it come up that anyone was scammed. And you mentioned that scamming was something that’s fairly common. Explain how it worked. I need this to take back to——

Mr. SCHWANKE. What they were doing was they were calling these victims and calling that area with those victims in it offering Federal grant money. So you would have thought——

Senator INHOFE. Well, pause right there. How would they expect money to be wired to them because—procedurally, how would that work?

Mr. SCHWANKE. I don’t know how they were going to get the money, and I don’t think that we had anyone fall for it in that area because it was reported.

Senator INHOFE. Oh.

Mr. SCHWANKE. But they were asking for that money. You would have had to have paid—you would have had to have paid an application fee in order to receive this free Federal grant money for rebuilding after the fires.

Senator INHOFE. Yes, that’s really, because that’s such a cruel thing. I mean, Mr. Abagnale, they were telling stories about how they were watching their livestock burn alive during this thing. It was really a tragedy, and that hasn’t come up as an issue in the meetings that we had. So I’ll maybe talk to you afterwards. And I want to visit with them out there because I’m sure if it was happening—it was taking place.

Mr. SCHWANKE. Well, and I want to give a lot of credit. That’s an example where local law enforcement stepped out so quickly on it. In these scams, you can’t wait on something like that a week or 2 weeks. They stepped out that day, called a news conference, and talked about it. So they were able to get that information out quickly, both through the news, but also the incredible tool that we have in social media, and it passed around very quickly.

Senator INHOFE. Yes. General DeWine, I remember so well recently, and you would have no way of knowing this, but OG&E, that’s in Oklahoma, Oklahoma Gas and Electric, they had their representatives make phone calls to customers and get them to make payments to the scammers. Is this something that has hap-
pened other places where utilities and this type of group out there would be involved in scamming?

Mr. DeWINE. Senator, I'm not—I don't have any specific recollection that we had one of those cases. You know, most of these cases come down to some representation to you that you're going to get something, you, the consumer are going to get something, and it's usually, as we tell people, if it sounds too good to be true, it probably is not true. But they all kind of follow that, you're going to get something, and to get something, we'll send you a check, but you have to send us a check type thing. And it could be the attorneys' fees or the cost of handling or something.

Senator INHOFE. Yes, well, maybe it's just particularly of concern in Oklahoma, but it did lead off into a lot of scams that were taking place just through that company.

Thank you, Mr. Chairman.

The CHAIRMAN. Senator Udall.

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

Senator Udall. Thank you very much, Chairman Moran. And I also want to thank the panel and the witnesses today. I think this has been excellent. And clearly this is a critical issue for the American public.

As State Attorney General in New Mexico, we brought many consumer protection cases in the areas that you all are talking about. One of them in particular was fraudulent telemarketers; we fought hard against them. These predators often targeted senior citizens. State Attorneys General were one of the key forces behind passing a Federal law that allows states to prosecute telemarketers who cross state lines, which I'm sure, Attorney General DeWine, you're familiar with.

Technology evolves and con artists adapt and deploy new techniques. Scammers also seem to quickly find ways to abuse Internet technologies. One example is credit card skimming.

Chairwoman Ohlhausen, drivers in Albuquerque have had their credit cards compromised after purchasing gas at a pump. Local TV stations KRQE and KOB have reported that Albuquerque police believe 22 credit card skimmers were recently installed at gas station pumps across the city. These skimmers are hidden and can be especially hard to spot if you're in a hurry to fill up your car with gas. And other skimmers are more sophisticated and read credit card information wirelessly, so you can just put them in a backpack, and I think there are pictures of those in front of you, both the first photo and the second photo, so: skimmers at a gas pump, and then the second one is a kind of skimmer that can get things wirelessly.

A Russian company sells this type of skimmer, the wireless one, and gives directions on how to steal credit card information. The Russian seller's website recommends targeting restaurants by hiding the skimmer in a backpack or in a car parked outside. This skimmer will, quote and they say in their advertisement “automatically connect to the network, can do all the job for you. You could probably get up to 20 card details from one restaurant depending on how busy the restaurant is.”
The FTC previously issued a warning to Americans traveling abroad to be alert for card skimmers at ATMs and gas stations, but these scams are now happening in New Mexico and across the Nation.

And so, Madam Chair, what action will the FTC take to help stop credit card skimming scams at the gas pump?

Commissioner OHLHAUSEN. Senator, thank you very much for your question. You raise a very important issue. In fact, it is happening across the country. And just locally recently WTOP reported that it was happening in Arlington, Virginia. And it is a problem, and we have issued consumer education for consumers, to tell them to be alert for things where it looks like it has been affixed overtop the regular card reader. And we give consumers advice about covering up with their hand as they’re putting in their PIN number. I certainly hope that as credit cards move toward the PIN and chip technology, that might help reduce the issue.

Now, you also raised the point about the websites selling this. I will certainly look into it. It’s possible that it could be reached under our unfairness authority. We have a three-part unfairness test. But one of the challenges is when things are sold abroad, it can be difficult sometimes for us to get authority over a foreign seller, but we can certainly see what we can find out.

Senator UDALL. Well, we hope you will work with the state attorney generals to try to shut these operations down.

Commissioner OHLHAUSEN. Certainly.

Senator UDALL. Now, for years, as you know, I’ve urged the FTC to take action against false marketing of so-called “anti-concussion sports equipment.” These false claims put children at greater risk of brain injury. And these false claims can put responsible companies at a competitive disadvantage. And tomorrow, in fact, is Brain Injury Awareness Day, and there is much greater awareness these days that concussions are a form of brain injury and should be treated seriously. So I was disappointed by President Trump’s tough guy comments at a campaign rally last year after an audience member fainted and then returned to the crowd, and he compared her favorably to an NFL player who sit on the bench after suffering a concussion. And Trump used to own his own professional football team, and he said, and I quote, These new and very much softer NFL rules, concussion, oh, oh, got to get a little ding on the head, no, no, you can’t play for the rest of the season, our people are tough. That’s the end of his quote. The President said that, I’m sure, for a laugh, but chronic traumatic encephalopathy, or CTE, and other forms of brain injury are no joke.

So, Madam Chair, are you aware that these current state laws and Federal health guidelines from the Centers for Disease Control recommend that athletes should not return to play immediately after a concussion?

Commissioner OHLHAUSEN. Senator, you raise a very, very important issue, and one that I care about deeply. I actually have four children, and two of them did suffer concussions playing sports. So I appreciate the attention that you’ve brought to this.

And at the FTC, we have brought enforcement actions in this case, the brain guard case. We’ve had consumer ed. I will continue to pay close attention to this issue. And I was also pleased to see
that the university is doing a study about the possibility of the concussions in the soccer—the sport of soccer. So we will definitely continue to pay attention to this issue.

Senator Udall. Yes. Thank you for that answer. Thank you for the courtesies. I know I ran over a little bit.

Thank you, Mr. Chairman.

The Chairman. You’re welcome, Senator Udall.

Senator Cortez Masto.

STATEMENT OF HON. CATHERINE CORTEZ MASTO,  
U.S. SENATOR FROM NEVADA

Senator Cortez Masto. Thank you, Mr. Chairman. And I apologize, I have dueling committees going on, so I just had to run over real quick.

First of all, let me say to my colleague, General DeWine, it’s good to see you.

Mr. DeWine. Good to see you.

Senator Cortez Masto. Had some important work we did together, and I thank you for continuing that work down the path of consumer protection.

And then, Mr. Schwanke, it’s important what you do. We have a station in Nevada, KTNV, that does similar work to protect consumers and bring education and awareness, which I think is one of the most important pieces protecting consumers, that education and awareness piece, and it’s the first step in prevention. So thank you for what you do.

I appreciate all the panelists here today.

And to the FTC, great partners of mine when I was Attorney General in the state of Nevada. Thank you for all of that hard work, because I do believe, as Chairwoman Ohlhausen has said, that the FTC is the primary consumer protection agency, so are the AGs, and when we have a partnership together, that is the most important thing. And so that’s where I would like to start.

And I really want to talk about and kind of get your position, Dr.—or excuse me, Chairwoman Ohlhausen, on your vision for the FTC. In your statement, upon your appointment as Acting Chair of the FTC, you stated, ‘I’m deeply honored that President Trump has asked me to serve as Acting Chairman of the FTC, and to preserve America’s true engine of prosperity, a free, honest, and competitive marketplace.’ And then on January 24, 2017, at the Heritage Foundation, you said, ‘Although well-intentioned, the majority Commission, under President Obama, at times pursued an antitrust agenda that disregarded sound economics. It imposed unnecessary costs on businesses and substituted rigorous analysis of competitive effects for conclusory assertions of unfair competition.’

With that said, I will tell you during that period of time, the FTC, they were wonderful partners of ours in the state of Nevada when we were addressing anticompetitive conditions in the marketplace that were there—we were there fighting to protect consumers.

So I’m curious, exactly which policies do you believe the Obama administration pursued that disregarded sound economics? And can you elaborate on that for me?
Commissioner OHLHAUSEN. Certainly. So in those remarks, I was talking about the FTC’s antitrust enforcement. For the most part, I supported it, I voted in favor of most of our enforcement, particularly in the pharmaceutical space, hospital mergers, challenging a wide variety of mergers. But there were a few cases that I didn’t support, and I filed dissents in those because I didn’t think that on balance they would make consumers better off, and I didn’t believe that the economic evidence supported finding an anticompetitive impact from that behavior that was being challenged.

Senator CORTEZ MASTO. OK. So can you commit that there won’t be a rollback of antitrust protections intended to protect consumers?

Commissioner OHLHAUSEN. I think that all of our antitrust enforcement definitely should protect consumers. I certainly wouldn’t want to forego any enforcement that I think has accurately shown there is a likely impact on consumers, an anticompetitive effect. And I’ve generally been very supportive of antitrust enforcement in those areas, or I would say hospital mergers, pharmaceuticals, mergers that raise problematic overlaps.

Senator CORTEZ MASTO. And have you spoken to the President or anyone else in the White House about your antitrust views?

Commissioner OHLHAUSEN. I have not spoken to the President. I have spoken to members of the White House staff.

Senator CORTEZ MASTO. OK. So to both commissioners, while I’m aware that the FTC’s authority does not specifically extend exclusively to banks, savings and loans, and Federal credit unions, you do work in concert with the CFPB. They were great partners of ours in the state of Nevada, as attorney general. How would you rate that cooperation in the CFPB’s ability to protect consumers?

Commissioner OHLHAUSEN. So we—once the CFPB was created, we reached a Memorandum of Understanding with the CFPB so that there weren’t inappropriate overlaps or burdensome overlaps, and we used our resources effectively. So I believe that we worked well with the CFPB. They worked in their area, and the FTC continued to operate in the areas that Congress left to us.

Senator CORTEZ MASTO. And do you think there is a good working relationship between the two of you in respecting those boundaries and then working together when necessary for consumer protection?

Commissioner OHLHAUSEN. I have not been aware of any problems with our relationship with the CFPB pursuant to the MOU.

Senator CORTEZ MASTO. OK. Thank you. And then to General DeWine. We have talked about this several times amongst our colleagues. But given the growing aging population, and you brought it up as well as constantly evolving technology that’s out there that you talked about, that we know that makes scams easier to perpetrate, what additional resources or innovations does law enforcement need to keep up with the financial threats posed to seniors?

Mr. DEWINE. Senator, I think that the biggest challenge is lack of resources and prioritizing. We have been successful in the Attorney General’s Office in helping local law enforcement. Ohio has a very local law enforcement; we’re county by county, 88 counties. And where we have been able to be successful I think is when we’ve been able to see a pattern of crime that goes from county to
county to county, and we get involved, and then we work with local law enforcement.

So I think it is, frankly, if there is one thing that is needed, it’s just more of that, more of that not only at the state level and the local level, but also with our partners at the Federal level. We work very closely every day with the DEA, with the FBI, other Federal agencies, but, again, as has been pointed out many times, when you have these cases that start, they’re on the Internet, some scammer may be sitting in halfway around the world, it’s a rare case, frankly, that we’re going to be able to be successful, and, quite candidly, I think what I would like to see is the Federal Government prioritize, we understand they can’t take every case, make some examples. It would be good just to have some high-profile cases where they say, “We’re going to go do what has to be done.” Because these scammers by and large are sitting offshore, and they don’t feel any heat.

Senator CORTEZ MASTO. Right.

Mr. DeWINE. They don’t feel any heat at all. So I think—I understand the lack of resources and prioritizing, and so maybe if we could do some of those cases for—you know, to make an example of them.

Senator CORTEZ MASTO. Thank you.

Mr. Chair, I see my time is up. Thank you for your indulgence. And thank you to the panelists.

And, Mr. Abagnale, thank you for coming forward with your insight and helping those of us to protect consumers. I appreciate it.

Mr. ABAGNALE. Thank you.

The CHAIRMAN. Senator Hassan.

STATEMENT OF HON. MAGGIE HASSAN, U.S. SENATOR FROM NEW HAMPSHIRE

Senator HASSAN. Thank you, Mr. Chair. And I’ll add my thanks to all of the panelists. Thank you for being here today on this really important topic. And I just wanted to follow up on something my colleague just talked to you all about because your testimony and certainly the experience of our constituents makes clear that our consumers are facing threats from bad actors pretty much across the board. We have Federal entities in place in addition to the FTC, the CFPB, which Senator Cortez Masto just referenced, the FCC.

So can you just—to the two commissioners here, can you talk a little bit about what you’re doing to make sure that there is excellent communication and coordination across the Federal Government on behalf of consumers? Are there any things in addition to what you’re already doing that are particular challenges or you need help with?

Commissioner OHLHAUSEN. So we do work closely with our Federal partners across the government, and we also as well as working with the states as much as possible. So we do a Memorandum of Understanding with a variety of Federal agencies. I mentioned CFPB. We have the FCC. We have the FDA. We participate in task forces. We’re a part of the Robocall Strike Force Task Force and the Identity Theft Task Force, so we do try to leverage our resources and work cooperatively.
Senator HASSAN. Thank you.

Commissioner?

Ms. MCSWEENY. I would just add that I think your point really underscores the need for strong consumer protection enforcement agencies to collaborate in order to make sure that we can adequately protect consumers in this environment. We really don’t see the threat to consumers or the marketplace diminishing, in fact, we see it increasing, and so what we need to make sure we’re doing is all using the tools that we have to do the best job that can do, and I think the FTC has been working hard to do that and will continue to do that, but we need to make sure that we have strong partners at the Federal level, at the state level, and in the business community as well.

Senator HASSAN. Thank you. And it has been part of my experience, as a Governor, that with all of this kind of law enforcement challenge, communication at all levels is just really, really important. So I appreciate your efforts.

This is a question for the entire panel. Mr. Abagnale today discussed how much easier it is to commit the kind of fraud you did as a teenager because of the proliferation now of new technologies, and to be sure, technology has played a tremendous role in enabling nefarious actors to commit schemes and to prey on innocent Americans.

So the question to all of you is technology is clearly part of the problem. Can it be part of the solution? And what should we be looking for it to do? Are state and Federal entities investing in the right kind of research and new technology that can help us prevent scams or identify them earlier? And can businesses help government do this?

Go right ahead, Mr. Abagnale.

Mr. ABAGNALE. I would just say absolutely. Technology can be used to fight crime. For example, as you know, a year ago the IRS paid out $5.8 billion in refunds to individuals who used someone else’s Social Security number. A simple technology that exists today and used by American corporations and banks every day in fraud detection would have prevented probably 70 percent of those payments being made. So the question is we have the technology, but it has to be used and it has to be implemented.

I work on retainer to LexisNexis on government risk solutions; have for years. I work on retainer to Experian, and they operate in 80 countries around the world. Obviously, I know the technology exists; I know we use it in the commercial marketplace. So yes, you can prevent a lot of these things from occurring by simply using the right technology to do so, but you have to be willing to spend the money and take the time and effort to do so.

Senator HASSAN. Right. Thank you.

Anyone else want to add?

Ms. MCSWEENY. I would just add one of the other ways we try to do that is by using our authority to run competitions to create new and innovative solutions to consumers. So in the past, we have used the authority to create apps that help consumers block unwanted calls, for example. Now we’re using it to create new tools to help consumers secure their home Internet of Things technology.
And that kind of entrepreneurial creative use of authorities can really spur innovation in the marketplace as well.

Senator Hassan. Thank you.

And, Commissioner, do you have anything?

Commissioner Ohlhausen. Yes. I just wanted to mention we at the FTC have tried to stay up-to-date on these things. We have an OTech, an Office of Technology, in our Bureau of Consumer Protection, and we also have a chief technologist at the agency.

Senator Hassan. Thank you very much. And, again——

Mr. DeWine. Senator, very, very quickly.

Senator Hassan. Yes.

Mr. DeWine. As I've traveled around the state, a lot of business people have been saying to me, “What are you doing about identity theft and other problems?”

Senator Hassan. Right.

Mr. DeWine. And, quite frankly, I went back to my office and I said I'm not sure really what we're doing.

Senator Hassan. Right.

Mr. DeWine. So what we have done is reached out to businesses and asked them to give us their best people literally to put on a group to start working on these issues. They're going to be coming out with a report fairly quickly. Our concern is not the big companies, they have the resources to do it, but the vast majority of companies in Ohio are small and frankly don't have the resources. So what we hope to do by getting people loaned frankly to us—and we've been very, very pleased with the quality of people the companies have given us, we think we're going to come up with some recommendations, maybe some legislation, best practices, that will help small business.

Senator Hassan. Great. Thank you very much. Thank you all.

Thank you, Mr. Chair.

The Chairman. Senator Klobuchar.

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

Senator Klobuchar. Thank you very much, Mr. Chair, and thank you to the Ranking Member as well for this important hearing. I apologize I was late. I was over at the Judiciary hearing, and I was telling Senator Moran I would use the very same tone and start asking you guys about things you wrote 10 years ago.

[Laughter.]

Senator Klobuchar. So many of the witnesses today have highlighted the growing problem of senior fraud. I introduced the Senior Fraud Prevention Act with Senator Susan Collins, the Chair of the Senate Committee on Aging, to help the FTC more effectively combat senior fraud. The bill was passed by this committee in January. Chairman, thank you for being here. One provision of the bill would establish an office within the Bureau of Consumer Protection focused on senior fraud. Have efforts to provide specialized resources for other targeted groups, like Spanish speakers, military consumers, and small businesses been successful?

Commissioner Ohlhausen. Thank you, Senator. We are very pleased to say that we also share your interest in focusing on fraud against seniors. We've developed a lot of consumer ed and help for
seniors in that area, we are doing the same for military, we have Military.Consumer.gov, and also for Spanish speakers. We think there are certain populations that might have particular needs, particular interests, and we want to reach out to them.

Senator KLOBUCHAR. Very good. Thank you.

Attorney General DeWine, thank you for being here. I wanted to hear more about your elder justice initiative. I actually embarked on such a thing when I was county attorney in Minnesota. And just one little aside, right after I announced it, 5 days later we started to prosecute an 88-year-old who had shot her boyfriend in the back, he survived, because she was mad he was dating someone else. And so people that were her friends accused me of that was my senior initiative. Of course, it was designed to help seniors. Could you talk about what you’ve done?

Mr. DeWINE. Well, thank you, Senator, very much. As you know, and the members of the Committee know, a lot of these scams are targeted specifically at elderly. And I think it has been this way forever. You know, there’s a reason that mature neighborhoods are targeted that have the older trees and the older citizens, for the tree scams, where they roll in and tell you that your tree is about to fall on your house. They’re doing it also more sophisticated now, of course, and that is through the Internet.

What we have done in the Attorney General’s Office is we have put together people from different parts of our office to really be kind of a strike force to respond when local law enforcement has a consumer instance where there has been elder abuse. Elder abuse, as you know, can be financial, it can be physical, and it also can be psychological. And what we find is that particularly the smaller jurisdictions simply do not have the resources to go after this, and sometimes it can take——

Senator KLOBUCHAR. Then you’re helping the smaller jurisdictions?

Mr. DeWINE. We’re helping the smaller jurisdictions, so we can bring forensic accountants in, for example, if we’re dealing with something having to do with fraud, money fraud. As I indicated, Ohio is a very local government state, and we like it that way, but what happens sometimes is the local jurisdiction just does not have the resources.

Senator KLOBUCHAR. OK.

Mr. DeWINE. The other thing that we really have tried to put an emphasis on is getting cooperation from the banks and other people who are dealing with the seniors on issues of money, and to inform them, educate them, that they can really be an advocate and stop some of this stuff right there.

Senator KLOBUCHAR. OK. Thank you.

Madam Chair, one last question along that issue of money and deception. I’m Chair with Senator Blunt of the Travel Caucus, Tourism Caucus, and one of the trends that we’ve seen to threaten this huge industry, of course, which has so many jobs in our country, and certainly as Senator Cortez Masto knows, is the rise of deceptive online companies that imitate the websites of actual hotels or airlines in order to attract bookings. These fraudulent websites can leave consumers with airline itineraries or reservations that have errors and they can’t be honored. That’s why Senator Fischer
and I wrote to the FTC to ask you guys to investigate the matter, and why Senator Daines and Nelson and I introduced the Stop Online Booking Scams Act. What actions has the FTC taken in this area?

Commissioner OHLHAUSEN. Senator, I am aware of your letter and appreciate you bringing that to the FTC’s attention. This is an important issue. We’re always concerned about deception for consumers. I can’t comment on whether we have any investigations ongoing, but we have looked into the issue and we’ve also issued consumer education on this.

Senator KLOBUCHAR. OK. Very good. Thank you. I am now returning because my colleague, Senator Franken, is asking his questions, which would almost be as exciting as yours, Catherine. So thank you, everyone. Thank you.

The CHAIRMAN. We’ll take a pause just for—right there, that length of time. We won’t take a pause any longer, although when he returns, I’ll be glad to—oh, he’s here. The Chair recognizes Senator Markey.

STATEMENT OF HON. EDWARD MARKEY, U.S. SENATOR FROM MASSACHUSETTS

Senator MARKEY. I apologize. I thought I was——

The CHAIRMAN. Senator Klobuchar was briefer than normal.

[Laughter.]

Senator MARKEY. Thank you. Commissioner McSweeny, last year the FCC wisely adopted broadband privacy rules that put consumers in control of their sensitive information, but now the broadband industry and their allies are fighting to strip away the fundamental privacy protections under the guise of harmonization of regulations. We could vote this week on a Congressional Review Act resolution rescinding these rules. When the industry says “harmonization,” they really mean self-regulation.

Commissioner McSweeny, in a recent op-ed, you stated that efforts to rescind the broadband privacy rules through the CRA process will not actually harmonize regulations, but create a, quote, yawning chasm where broadband and cable companies have no discernable regulation. Could you explain?

Ms. MCSWEENY. Thank you, Senator, for the question. The point that I’m trying to make is that both the FTC and the FCC have an important role to play in making sure that people have choices and control over their sensitive personal information. And in the always-on, always-connected environment that we now live, those choices are even more important than ever. Something like 91 percent of American consumers feel they have lost control of their data. So rather than rolling back rules that simply guarantee that they get a choice, we should be doing everything in our best efforts both at the FTC and at the FCC and other parts of the government to protect those choices and guarantee them.

Senator MARKEY. So should we be allowing broadband companies to collect, to use, to sell sensitive information about subscribers’ health, finances, and children without first getting consent from those families?

Ms. MCSWEENY. Well, the FTC’s perspective over 20 years of protecting consumer privacy——
Senator MARKEY. No, I'm talking about the Federal Communications Commission.

Ms. MCSWEENY. Right. And——

Senator MARKEY. Those rules should stay on the books.

Ms. MCSWEENY. I strongly support those rules because they are consistent with what the FTC has required, which is choices be offered to people before their sensitive information is used.

Senator MARKEY. Thank you. A last-minute provision in the 2015 budget deal makes it easier for government debt collectors to harness tens of millions of consumers on their mobile phones. And last summer, the Federal Communications Commission, in response to a Supreme Court ruling, exempted the entire Federal Government and its contractors for key robocall protections.

This carve-out for government robocallers coincides with a rise in tax and debt collection scams where criminals posing as IRS agents and debt collectors call innocent Americans telling them they must promptly wire them money or be subject to arrest, deportation, or revocation of driver licenses. Americans have lost millions of dollars because of these scams.

A provision in the 2015 Surface Transportation Bill actually encourages the IRS to hire private debt collectors to collect certain unpaid taxes, private tax collectors that can now robocall and robotext consumers without their consent. I'm concerned that consumers could find it even more difficult to detect fraudulent calls because of these recent actions.

Commissioner McSweeny, Commissioner Ohlhausen, do you agree with me, that there should be much concern about this change in law?

Commissioner OHLHAUSEN. Senator, when the FCC proposed a Notice of Proposed Rulemaking about government debt collection, the FTC's Bureau of Consumer Protection did file a comment raising some concerns. And when the FCC adopted the final rule, they did adopt several of the recommendations that the FTC staff had included, that things such as limiting the duration of the call, excluding any calls from that coverage that would have any marketing, requiring callers to affirmatively inform debtors of their right to make the request to stop calls. So I did share those concerns, and I was pleased to see that the FCC took those into account in the final rule.

As for the IRS plan to use private debt collector contractors, I think it will raise an additional informational challenge and educational challenge for the FTC as they tell consumers how to be wary of imposter scams.

Ms. MCSWEENY. I would just add I agree. I think consumer confusion here is a very strong possibility, and that could be problematic, and that our second most prevalent complaint is bad debt collection practices, and to the extent that we have debt collection occurring, we need to make sure that rules are followed that protect consumers' interests in those proceedings.

Senator MARKEY. Thank you. And earlier this month, Senator Lee, from Utah, and I introduced the bipartisan HANGUP Act, the Help Americans Never Get Unwanted Phone Calls Act. The bill closes these loopholes and ensures that consumers do not receive
unwanted robocalls and robotexts from Federal Government contractors without consent.

Last year, the FTC received over 5 million complaints about unwanted calls. In light of this high volume of consumer complaints, would you support our legislation, Senator Lee and I—the HANG-UP Act?

Commissioner OHLHAUSEN. Senator, I haven’t seen the Act. I would certainly be happy to take a look at it, and I share the goals of that Act. I am concerned about consumer complaints, and it’s something we have paid close attention to at the FTC over the years.

Senator MARKEY. Commissioner McSweeny?
Ms. MCSWEENY. I agree.

Senator MARKEY. OK. Thank you.

I am the original House author of the Telephone Consumer Protection Act. And I’m going to oppose anything that undermines these fundamental protections, which people want in their homes from unwanted invasions of their privacy and compromise of information that is sensitive to their families.

So I thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Markey.

I have just a couple of wrap-up things. Maybe we can get this concluded quickly. It’s terribly warm in here. But you all never took your coats off, so I left mine on.

Mr. Abagnale, is there any level of cooperation between those protecting consumers here in the United States and those abroad? What we heard today was a lot of things are beyond our reach, and what you indicated was the best opportunity we have is to prevent through education and consumer awareness and the actual enforcement, the ability to—the Attorney General said something very similar, the actual ability to prosecute, to put somebody out of business, or to get the funds restored is pretty limited, and I assume in part that’s because we no longer know the person who is perpetrating the fraud. I would guess in most instances there is no, any longer, any relationship between the victim and the perpetrator. Is that true?

Mr. ABAGNALE. That’s true. And I think that there are, of course, some countries that we’re able to have cooperation with and be able to use enforcement tools to stop those individuals or arrest those individuals, but when you look at most of these scams that come over the phone, they’re coming out of China, they’re coming out of India, they’re coming out of Russia. We have gangs in Russia that bring in about $20 billion a year annually from these types of scams and crimes that are committed by these gangs, and there aren’t a lot of American companies that make $20 billion a year tax-free in that case.

So I think there are some countries that we can work with. When I get calls—and what I wanted to comment on earlier is when people ask me, “I’ve been a victim. Where is the best place for me to call?” I always tell them the Attorney General of their state and to the office of their consumer protection. They’re the ones who really do the most about these things. They’re the ones who have the tools to help with those problems. So I always direct them there first.
Unfortunately, the FBI, as you know, has only 13,000 agents, and obviously those agents are dealing with kidnappings and counterintelligence items and things of that nature, so those crimes get to where there is a dollar amount has to exceed that amount before there is an investigation, and the U.S. Attorney only prosecutes when it exceeds a certain dollar amount. And I understand why that is done.

So it’s best to probably try to deal with those things on the local level with the Attorney General and then get the cooperation when we know that someone might be out of state or somewhere we need Federal law enforcement to help investigate or apprehend that individual.

The CHAIRMAN. Are there any successful instances in which the Internet provider or the phone carrier or the company has acted in a way that then shuts down or prevents additional fraud?

Mr. ABAGNALE. Well, what happens, if the phone company was to shut down a phone number tomorrow, it’s just a throw-away cell phone, so they just have hundreds and hundreds of phones, and so a new number is a couple of seconds away, so it’s very difficult to do that.

I would encourage, again, there probably is ability with technology to—phone companies could use to track a lot of those calls and then stop those calls from coming into an individual number, but I don’t know that there is anyone really doing that at this time.

The CHAIRMAN. From an FTC point of view, where are you in the FY18 budget request? Anything transpiring in regard to what request the administration will make for your agency?

Commissioner OHLHAUSEN. So we weren’t mentioned specifically in the President’s, quote, skinny budget, so we’re still waiting to see exactly how we’ll be treated.

The CHAIRMAN. And let me ask while I’m visiting with you, Madam Chairman, it was mentioned earlier in Senator Blumenthal’s opening statement about the BOTS Act, that this subcommittee and full committee passed and was signed into law by the President, designed to rid us of the so-called ticket BOTS, who automatically have the ability to corner the market.

Commissioner OHLHAUSEN. Yes.

The CHAIRMAN. What’s the status of—any complaints, any inquiries made to the FTC, in regard to that law?

Commissioner OHLHAUSEN. So I commend you for passing the Act. And we are currently talking to people and finding out if there are complaints that we can act upon.

The CHAIRMAN. So nothing at this point. I mean, give me a little more detail of what that means.

Commissioner OHLHAUSEN. So our staff is reaching out to other entities, other enforcers, finding out if there are violations of the Act ongoing and how we would track them down, finding out if there are consumer complaints, and using our usual tools to investigate whether there is a violation that we could pursue.

The CHAIRMAN. Attorney General, that legislation also allows for state enforcement. And I would highlight that legislation for you, and maybe you’re aware of it, but the opportunity to try to rid us of those automatic acquisition of tickets then sold to, I don’t know,
Buckeye games or something that may be popular. Are you aware of that?

Mr. DeWine. No. I'll take a look at that. Thank you, Mr. Chairman, very much.

The Chairman. Thank you very much.

Mr. Abagnale, tell me a bit, I'll give you a chance to talk about perhaps your sponsor or your host, the AARP. So what is it that I can do with Kansans with AARP to further highlight how to avoid being scammed?

Mr. Abagnale. You know, it's interesting, I have spent most of my career dealing with crimes against businesses, business-to-business crimes, but I was well aware of all these consumer issues. Most of my time has been spent dealing with those crimes. A few years ago, AARP contacted me and asked me if I would work with them in helping educate their members and non-members about these scams that are being perpetrated, how they're done, and how to prevent them.

I found toward the end of my career that this would be something really worthwhile for me to do and spend my time helping consumers instead of just businesses deal with crime. And it has been absolutely amazing. Over the last few years, I have talked to people who have lost their life savings, 80 years old, they've lost their home, they lost their car, due to some scam.

But I have found that the reach of the Fraud Watch Network to over 50 million people, the ability for me to go out and get on a phone and speak to 15,000 people on one phone call and reach those people and answer those questions, and when I do go out and do a presentation somewhere, the AARP does not allow for the sale of any items, they do not allow the promotion of their company, and they allow anyone to attend. So you don't need to be an AARP member.

And we're amazed that when we sit there watching the people come in, and we get crowds of 1,500–2,000 people, we notice that a lot of them are people in their twenties and in their thirties, and then married couples that are very young, and we ask them later why they came, and they say, "Because I'm concerned about my identity being stolen, and I'm concerned about my information being taken or being scammed myself."

So it has been a great way to reach people, and I will continue to do so this year to reach consumers en masse and be able to help them understand these issues and how to help protect themselves.

I would like to add one thing that I didn't get to comment on earlier. I am very concerned about children's identities. If you are selling an identity on the black market today, and you told me in Envelope A I have a 62-year-old male who is a multi-millionaire, owns hotels, restaurants, office buildings, shopping malls, and I'll sell you his identity complete, or I will sell you the identity of a 12-year-old that's in junior high school and has no credit or any assets, I would take the 12-year-old. And the reason for that is that if I can become that 2-year-old, that 5-year-old, that 12-year-old, I can become that person for a long period of time before that person will ever realize I stole their identity.

So when I was a child, you didn't get your Social Security number until you got a job, so you were 16, 17 years old, only three
people knew it—the government, your employer, and you. Today, you don’t leave the hospital without that number, and if I can get that number as that child leaves that hospital or shortly thereafter, that means I have 18 years of reselling, reusing that identity of that child before anyone else would know that. So I think we need to start paying a little more attention. It’s not just the elderly, but it is also children’s identities that are very much at risk, and we need to be able to try to come up with some solutions for helping those individuals.

The CHAIRMAN. There are increasing examples of fraud against Federal agencies and departments. Anybody have any feel for what that’s like? And are there departments that are taking the necessary steps to prevent that?

Mr. ABAGNALE. That’s my area, and it’s quite amazing. I used to tell people that I worked in the millions, but I only work in the billions now. So last year, Medicare and Medicaid paid out $100 billion in fraudulent claims, that was 10 percent of their combined budget. So we mentioned earlier the IRS paid out $5.8 billion in fraudulent tax returns that people filed using someone else’s name, $7.7 billion in fraud from unemployment fraud, and almost $10 billion in fraud from food stamp fraud.

This is billions and billions of dollars that in many cases leaves our country because it’s being stolen and benefits collected from people who are not even citizens or in this country. And what bothers me most about that is we have the ability to prevent a lot of that.

So I know that in the private industry, you have a board of directors, and you have shareholders, and you have a profit to make. Inside the government, that’s not there, so consequently the criminals start to realize, “Who has all the money?” The government: Federal, county, state, and city. And, “Who’s the easiest target?” Unfortunately, the government, because they don’t have the proper infrastructure in place, let’s say, for example, Chase Bank, that spends more than $600 million a year to put technology in their bank to keep criminals out of their bank.

So I would like to see the Federal Government, even if you were to cut those losses by 20 percent, 25 percent, that’s billions of dollars that go back into building roads, helping the homeless, and people who need that money. So I think the government can do a better job of preventing a lot of the crimes that are perpetrated against them; they just need to take the time, the money, and the effort to do so.

The CHAIRMAN. I also serve on the Appropriations Committee, and it has been one of our standard questions to ask agency heads, Cabinet secretaries, chief information officers, “What is it that you’re doing to protect the data that you have authority over?” and we’re trying to improve the status. I hadn’t thought about states and local units of government, but it would be the same kind of challenge that we have.

One thing you said today, among many others that was said by all of you that stands out with me, I thought about the consequences of fraud or scams and the economic loss to the victim. What you said, Mr. Abagnale, that will stick with me is the consequences of the money then coming back and used in different
ways so damaging to our society, more than just a personal loss, the volume, the amount of dollars, that are accumulated can be used in nefarious and damaging ways.

Mr. ABAGNALE. Absolutely.

The CHAIRMAN. Ms. Cortez Masto?

Senator CORTEZ MASTO. Mr. Chair, thank you. And let me just add because I completely agree, as somebody who oversaw the Medicaid Fraud Unit for the state of Nevada. It was so important to put resources into the staff, both the prosecutors and investigators, who can investigate and prosecute for that fraud. One case alone we were able to put $2 million back into the Medicaid system.

So part of this process I believe is also funding those inspector generals or funding those agencies and their units within those agencies that can continue to go after the type of fraud and keep that money in the system to the benefit of the people who really need it. So I appreciate those comments. Thank you very much.

The CHAIRMAN. Thank you very much. Anyone have anything they want to add that they felt like they didn't get the chance to make because I was inarticulate in my questions?

Mr. Schwanke.

Mr. SCHWANKE. Real quickly, on the IRS law that’s going to allow the collection via phone that was brought up, I can tell you that I would have significant concern as over the past few years that’s all we have done was try to educate consumers that the IRS will not call you. I think I echo concerns of the BBB that I talked to here, that there will have to be significant reeducation happening because over and over again we have told viewers that the IRS will not call you to collect any tax debt. So as—and the IRS has also gone on our air many times saying that. So that would be a concern.

The CHAIRMAN. And another takeaway from the hearing for me is the lack of emphasis or the declining emphasis on public service announcements awareness campaigns that was described as used to be more prevalent than it is today.

Anyone else?

Mr. DeWINE. Mr. Chairman——

The CHAIRMAN. General.

Mr. DeWINE.—just one last thing to follow up on what Mr. Abagnale said in regard to young people and the identity theft of young people. One of the things that we've done in Ohio is pass a law that provides that a parent can go to the credit reporting agencies and actually freeze that child's credit, and once that credit is frozen, then obviously it is not as beneficial for someone to steal it, and if they do steal it, there is not a whole lot they can do with it, or not as much. So that’s one thing that we’re doing in Ohio and we think can help.

The CHAIRMAN. Thank you very much.

Mr. Schwanke, you’re the Kansan on the panel; therefore, you’re the expert. Anything you want to make certain I know before I conclude this hearing?

Mr. SCHWANKE. I would just say we’re getting—I think there has to be better communication from government agencies to private businesses, not that there has to be more regulation, but we’ve
seen drastic improvement really over the past year or two. It was brought up by one of the members of up here that when they go to the banks or when they go to these businesses, especially the senior citizens, to withdraw money, or in my example, purchase $13,000 in iTunes cards, that a lot of times private business, through their education efforts, can stop this. That same grocery store that had that happen now has had multiple cases where their clerks have stopped the scam from happening, as have banks.

Banks in the past I think have been concerned with privacy, not prying into people’s personal lives and finances when someone comes to withdraw $20,000 cash, but I think that’s getting better that they’re able to ask some of those important questions to seniors when they go to make those type of withdrawals, whether it be a gift card or a cash withdrawal from a bank.

The CHAIRMAN. You and I both grew up in small towns, and you’re too young to know this, but in days gone by, everybody knew each other, and you knew when somebody might be doing something that made no sense to you, and you had enough of an awareness of their lives, their person, and their family, that you were willing to say, “Are you sure you know what you’re doing?” And we have fewer of those personal barriers and opportunities in today’s global economy.

Thank you all very much. We appreciate the time that you’ve spent with us this afternoon. We appreciate the education that we’ve received. This hearing record will remain open for 2 weeks. During that 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. And with that necessary announcement, I bring this hearing to a conclusion. Thank you all very much.

[Whereupon, at 4:26 p.m., the hearing was adjourned.]
Dear Senator Fischer,

As a Member of Congress who hails from a state that relies heavily on the travel and tourism industry – specifically 456 properties, 39,729 hospitality jobs and $4.6 billion in business sales in the state of Nebraska – I am writing regarding the upcoming hearing on the issue of offline hotel booking scams, for which there is a committee hearing, “Staying A Step Ahead: Fighting Back Against Scams Used to Defraud Americans” scheduled for March 21, 2017.

Each year thousands of travelers are misled into making hotel reservations through fraudulent websites and call centers that give the appearance of being connected to a hotel, but are actually imposter websites and call centers posing as hotels. In the last year alone, close to 15 million reservations were made on such imposter booking sites, resulting in hotel guests finding themselves out hundreds of dollars for either a worthless reservation or one that delivered much less than promised. It is estimated that these scams cost U.S. travelers upwards of $1.3 billion per year. The Federal Trade Commission has taken action to combat this problem by warning consumers and business travelers and led to scam alerts by AAA and the Better Business Bureau (866). See attached warning from the Federal Trade Commission.

In fact, in a recent survey of our state’s General Managers, we have heard many stories of multiple customers defrauded traveling to Nebraska, including the following testimonial:

**Microtel Inn & Suites, Kearney, Nebraska**

**David Hall, General Manager**

“Over the past year, at least a couple of guests have talked to me and we’ve reported the fraudulent website. There is an email I sent last year to our state attorney general’s office.”

As the general manager of Microtel Inn & Suites here in Kearney, NE, I’m becoming aware of reservation scams. Last week I had a guest who had searched for our hotel on their phone and came up with what they thought was our hotel and had called to make a reservation. They answered the phone as if they were with Microtel and when they mentioned that it would be $21 to make the reservation, it set off a red flag and she didn’t continue with the reservation. She showed me her phone and the number she called was 888-697-3743 and the website was hotelrates4.com. However, today, I had a guest inquire about the $50 off her first night. Again, as she was traveling down the interstate, (which is a lot of our business) she googled Microtel in Kearney and came up with an 888-935-1875 to make her reservation. Once again, it looked like a real hotel but she knew she wasn’t talking to our hotel as they had said they were Microtel central reservation. This time they offered her an opportunity to save $50 on her first night’s...”
stay. It was only $16/month. She asked me about her $50 off and I said I wasn’t aware of any promotions like that. The company was Travelers Advantage 800-568-1136, and a quick search shows there are plenty of complaints out there. I’m not sure how these companies are getting by with this and I sure hope to see guests taken advantage of. I’ve contacted Wyndham Worldwide (the hotel group that we are franchised with) about both of these instances. I’m not sure there is a lot you are able to do about this, but I felt I needed to make you aware. As traveler patterns have changed, hotels along the interstate are depending on their guests being able to use their mobile device to not only find us, but to make their reservations with confidence.

As Americans, we cannot stand by and allow travelers to be scammed by rogue websites – it harms our state’s tourism industry and reputation, and creates incredible hassles and financial loss for our customers. We commend you for putting a focus on the real-life issue of consumer scams, and ask that you work with the appropriate government and law enforcement agencies, and allow for proper punishment of these rogue websites and restitution for their victims.

Thank you for your attention to this critical matter,

Scott Merritt
Executive Director
Nebraska Hotel & Lodging Association
Did you book that night at the hotel’s site?
July 14, 2015
by Amy Intelisano
Consumer Education Specialist, FTC

Whether you travel a lot or just a little, you’ve probably been online to book a hotel stay. Sometimes you might find a travel comparison site gets you the best deal. Other times, you might book directly at a hotel’s website—maybe to earn points for the company’s rewards program, or because you have some special requests for your stay.

For those times you’re looking to book directly with a hotel, make sure that’s what you’re doing. The FTC has heard from people who searched online and thought they were booking on a hotel website, only to find they unknowingly were doing business with someone else.

The confusion resulted in problems like:
- Harassing and feeling no reservation
- Having trouble canceling or modifying a reservation, or
- Disputing charges through the hotel
- Finding reserved rooms didn’t reflect special requests like dietary access
- Being charged undisclosed fees
- Paying a higher rate than what’s advertised in the hotel
- Getting credit card charges from the third party, not the hotel
- Not earning points with the hotel’s rewards program

It can be hard to tell that you’re not on the hotel’s site. You might see a hotel’s name in the URL, or call the number shown next to the hotel’s address and not realize it’s the reservation company — not the hotel — you’re talking to.

Your best bet is to avoid surprises — look closely at your search results. If you know you want to deal directly with a hotel, take the time to look for signs you might be on a third-party site. Ask another company’s logo. It’s also a good idea to find the hotel’s phone number yourself, rather than rely on what’s listed on the site.
Did you book that night at the hotel’s site?

July 14, 2015
by Amy Hackett
Consumer Education Specialist, FTC

Whether you travel a lot or just a little, you’ve probably gone online to book a hotel. Sometimes you might find a travel comparison site gets you the best deal. Other times, you might book directly on a hotel’s website — maybe to earn points for the company’s rewards program, or because you have some special requests for your stay.

For those times you’re seeking to book directly with a hotel, make sure that’s what you’re doing. The FTC has heard from people who searched online and thought they were booking on a hotel website, only to find they’ve unknowingly been doing business with someone else.

The confusion resulted in problems like:

- earning and redeeming no reservations
- having trouble canceling or modifying a reservation, or dropping charges through the hotel
- finding reserved rooms didn’t fulfill special requests like dietary access
- being charged unexpected fees
- paying a higher rate than what’s advertised to the hotel
- getting credit card charges from the third party, not the hotel
- not earning points with their hotel rewards program

It can be hard to tell that you’re not on the hotel’s site. You might see a hotel’s name in the URL, or call the number shown next to the hotel’s address and still receive the reservation company — not the hotel — you’re talking to.

If your hotel is small or new, it can be a hard sell to get all your search results. If you know you want to deal directly with a hotel, take the time to call the hotel; you might see its website on a third-party site, with another company’s logo. It’s also a good idea to find the hotel’s phone number yourself, rather than rely on what’s listed on the site.
Question 1. You have stated your interest in combating scams as a top priority for the FTC’s Bureau of Consumer Protection. What specific practices do you intend to target? Can we expect to see increased FTC enforcement activity in this area?

Answer. Fighting fraud is at the core of the FTC’s consumer protection mission. Our anti-fraud program tracks down and stops some of the most pernicious frauds that prey on U.S. consumers, often on those who can least afford to lose money. The Commission will target the most egregious scams that cause significant economic injury to consumers, including imposter scams, such as government and business imposters; tech support scams which may disproportionately impact the elderly; robocall and other telemarketing scams; fake debt relief services and phantom debt collection schemes; and miracle cure scams. The agency also will work to combat scams that defraud small businesses, such as fake business directory services, as well as scams that deceive aspiring entrepreneurs, including business opportunity scams. I also will increase our efforts to fight scams that target members of the military and veterans.

Question 2. At the hearing, you testified that the annual macroeconomic cost of scams to the U.S. economy is “billions and billions of dollars.” Apparently, you based this figure on the redress FTC received in 2016, which included a settlement order the Commission secured against Volkswagen Group of America in excess of $10 billion. Presumably, however, this redress represents only a small fraction of the total cost of scams to the economy.

a. Has the Commission’s Bureau of Economics examined these costs? If so, what conclusions did it reach?

Answer. Over the last 15 years, the Bureau of Economics has conducted three surveys to study the degree to which consumers are affected by consumer fraud. Because of the limitations of the data available to the Bureau and other resources constraints, these studies researched the number of consumers affected by fraud, but did not address the question of the total costs such frauds impose on the economy.

The most recent survey, which was conducted in 2011, asked about 15 specific types of fraud, as well as two more general types.1 The types of fraud included in the survey are among the most common frauds perpetrated by mass-market fraudsters, based on information gathered from consumer complaints submitted to the Commission’s Consumer Sentinel database and Commission enforcement actions.

The 2011 survey found that 10.8 percent of U.S. consumers polled—which translates to an estimated 25.6 million American adults—had been victims of one of the frauds about which the survey asked.2 The most frequently experienced of these frauds were weight loss products that were marketed as making it easy for consumers to lose weight or as enabling weight loss without diet or exercise, and that did not deliver what consumers had expected. An estimated 2.1 percent of American adults had purchased such weight loss products during 2011. Fraudulent prize promotions—a situation where a consumer paid money, purchased a product, or attended a sales promotion to obtain a promised prize and then did not receive the prize or found that the prize was not what they thought they had been promised—was the second most prevalent of the studied frauds, having been experienced by an estimated 1.0 percent of U.S. consumers.

b. Do you believe it is important to establish a baseline of the economic impact of scams to assess the effectiveness of FTC’s enforcement and education efforts?

Answer. To fulfill its goal of protecting consumers, the FTC must identify consumer protection problems and trends in the fast-changing, increasingly global marketplace. The agency strives to understand the issues affecting consumers, including any newly emerging methods of fraud or deceit, so that it can target its enforcement, education, and advocacy on those areas where consumers suffer the most


2 In at least some cases, the figures that result from the FTC’s survey likely underestimate the prevalence of fraud. This is because fraud here involves paying for a product or service that the consumer had not agreed to purchase. This could occur, for example, if a consumer was deceptively offered a free trial of some service—perhaps a buyers’ club—and the seller then converted the free-trial to a regular paid subscription if the consumer did not cancel the membership during the free-trial period. (These types of offerings are often referred to as “negative option” offers.) However, if the charges just appear on consumers’ credit card or telephone bills and consumers do not realize that the charges are unauthorized, they will not be able to correctly report that they have been victimized.
A number of external factors pose significant obstacles to establishing a baseline of the economic impact of scams. For example, many injured consumers do not report when they have been harmed, whether out of embarrassment or for other reasons, and some consumers may not even realize that they have been victimized.

Nevertheless, I do believe it is important for the Commission to attempt to measure the economic impact that its enforcement and education efforts have on consumers and the economy, and the agency does set performance goals that can be used as a proxy for consumer harm. For example, in the FTC’s current strategic plan, the agency has set baselines from past performance, as well as goals designed to improve that performance. These baselines and goals apply several different measures, including the percentage of the FTC’s consumer protection law enforcement actions that targeted the subject of consumer complaints to the FTC; the total estimated consumer savings compared to the amount of FTC resources allocated to consumer protection law enforcement; and the amount of money the FTC returned to consumers or forwarded to the U.S. Treasury. The agency also has set performance measures for providing the public with knowledge and tools to prevent harm to consumers. For example, the agency has set performance goals for the rate of consumer satisfaction with FTC consumer education websites; the number of federal, state, local, international, and private partnerships to maximize the reach of consumer and business education campaigns; the number of workshops and conferences the FTC convened that address consumer protection problems; and the number of consumer protection reports the FTC released.

Question 3. In April 2016, the American Medical Association adopted a resolution supporting a “requirement that attorney advertising, which may cause patients to discontinue medically necessary medications have appropriate and conspicuous warnings that patients should not discontinue medications without seeking the advice of their physician.” Could attorney advertising, which induces a patient to stop taking a prescribed medicine, be actionable under Section 5 of the FTC Act? Has the Commission examined any recent cases involving such advertising, and has Commission staff been in contact with the American Medical Association and the American Bar Association regarding this matter?

Answer. Section 5 of the FTC Act prohibits “unfair or deceptive acts or practices in or affecting commerce.” 15 U.S.C. § 45(a). Whether the advertising that you describe would constitute an unfair or deceptive act or practice is a factual question that can only be answered on a case-by-case basis. However, I am happy to provide a general overview of the factors the Commission would consider in making such a determination.

The Commission has explained that a deceptive act or practice is a representation, omission, or practice that is likely to mislead a consumer acting reasonably under the circumstances and that is material. 3 If a representation, omission, or practice targets a particular group, the Commission will examine reasonableness from the perspective of that group. Further, a representation, omission, or practice is material if it “is likely to affect the consumer’s conduct or decision with regard to a product or service.” 4 Pursuant to Section 5(n) of the Act, an act or practice may be deemed unfair if (1) it “causes or is likely to cause substantial injury to consumers”; (2) the injury “is not reasonably avoidable by consumers themselves”; and (3) the injury is “not outweighed by countervailing benefits to consumers or competition.” 15 U.S.C. § 45(n). 5

The first element of unfairness is that the act causes or is likely to cause substantial injury to consumers. Accordingly, an inquiry would consider how likely is it that a particular ad would cause consumers to discontinue their medication and what consequences would likely follow if that happened, in order to obtain an overall understanding of the level of risk and harm to which consumers are exposed in a particular case. These factors would likely vary depending on the particular claims made in the ad, as well as the type of medication at issue.
The next element asks whether the injury would be reasonably avoidable by consumers themselves. Again, the answer to this question would likely depend on the claims made in the advertising, the medication involved, and the condition at issue. The final element is whether the consumer injury is outweighed by countervailing benefits to consumers or competition. Attorney advertising advising consumers who might have suffered injury to seek legal consultation can serve an important public purpose. Moreover, required disclosures impose at least some cost on advertisers. However, when there is a substantial injury to health, or the likelihood of such injury, that is not reasonably avoidable by consumers, a cost-benefit analysis will generally favor disclosure, if such disclosure will mitigate the injury. At this point in time, no specific cases involving patients discontinuing medically necessary medication in response to attorney advertising have been brought to our attention. We plan to contact the AMA to request additional information.

**Question 4.** Under Democrat leadership, the FTC sought to introduce novel harms into its “substantial injury” analysis, for example recognizing intangible harm as the basis for unfairness cases. A prime example of this is in the FTC’s LabMD enforcement, which you supported. Previously, the Commission tended to find substantial injury in cases of actual or likely economic harm, and in other instances, where physical health and safety is threatened.

a. Do you agree that the Commission should consider intangible harm as part of its unfairness analysis?

Answer. In order to effectively and efficiently protect consumers, the FTC must focus its enforcement efforts on stopping conduct that causes or is likely to cause substantial consumer harm. Public exposure of sensitive information of the type frequently used to facilitate identity theft can be likely to cause substantial economic injury. And it may create a significant risk of a concrete harm, which the Commission has also long considered to constitute substantial injury. Furthermore, the Commission’s longstanding view has been that an invasion of a consumer’s highly sensitive medical information can itself constitute an actual, concrete consumer harm under the FTC Act.

I do believe, however, that the FTC needs to examine more rigorously what constitutes substantial injury in privacy cases. This is one of the reasons I have asked the FTC’s Bureau of Economics to study the economics of privacy and data security. I expect that this work will help ensure our data security and privacy program stands on a strong policy foundation.

b. If economic or physical harm is not required, what is the predictable limiting factor on the types of harm that will result in enforcement?

Answer. As required by the first prong of Section 5(n) of the FTC Act and noted in the Unfairness Statement, the harm in question must constitute a substantial injury. Trivial, speculative, or certain subjective harms, such as those that offend the tastes or social beliefs of particular consumers, do not meet the first prong of Section 5(n). Unfairness Statement, 104 F.T.C. at 1073. In addition, for there to be a violation that may result in enforcement, the other prongs of Section 5(n) must also be satisfied, i.e., the harm must not be reasonably avoidable by consumers or outweighed by countervailing benefits to consumers or competition.

**Question 5.** In the FTC’s recent enforcement action in the matter of Vizio, Inc., you supported Count II of the complaint, alleging that Vizio deceptively omitted information about its data collection and sharing program, stating that “[e]vidence shows that consumers do not expect televisions to collect and share information about what they watch.” On this basis, you found that the company’s omission to be material, because “[c]onsumers who are aware of such practices may choose a different television or change the television’s settings to reflect their preferences.”

Could, and if so, should, the FTC apply a similar theory of deception to data collection and sharing in other contexts—for instance by Internet service providers, websites, or applications—with consumer may have lower expectations about the treatment of their data?

---

5 Unfairness Statement n.12.

Answer. Any determination of whether a specific act or practice is deceptive is a factual question that must be made on a case-by-case basis. As noted above, a deceptive representation, omission, or practice is one that is material and likely to mislead a consumer acting reasonably under the circumstances. A representation is material if it is likely to affect the consumer’s conduct or decision regarding the product or service. As explained in the Commission’s Deception Policy Statement, in making such a determination, the Commission will analyze the “net impression” of the representation being made from the perspective of a reasonable consumer.

The Commission has previously challenged deceptive omissions in other contexts involving data collection and sharing. For example, in *Goldenshores Technologies*, the FTC alleged that the makers of a popular free flashlight app deceived consumers about how their geolocation information would be shared with advertising networks and other third parties. While the company’s privacy policy told consumers that any information collected by their Brightest Flashlight app would be used by the company, it deceptively failed to disclose that the app transmitted users’ precise location and unique device identifier to third parties, including advertising networks. Likewise, in its case against *Epic Marketplace*, the FTC settled charges that the online advertising company used “history sniffing” to secretly and illegally gather data from millions of consumers about their interests in sensitive financial issues ranging from fertility and incontinence to debt relief and personal bankruptcy. According to the complaint, while Epic did disclose its privacy and behavioral advertising practices, it deceptively omitted that it engaged in history sniffing. Finally, in *Sears Management Corp.*, the FTC settled allegations that the company failed to disclose adequately the scope of consumers’ personal information it collected via a downloadable software application. Sears allegedly represented to consumers that the software would track their “online browsing,” but only disclosed the full extent of the tracking in a lengthy user license agreement, available to consumers at the end of a multi-step registration process. According to the FTC, the software would also monitor consumers’ online secure sessions—including sessions on third parties’ websites—and collect information transmitted in those sessions, such as the contents of shopping carts, online bank statements, drug prescription records, video rental records, library borrowing histories, and the sender, recipient, subject, and size for web-based e-mails.

*Question 6.* On December 14, 2016, the Consumer Review Fairness Act became the law of the land. This legislation, which I introduced in the Senate, addresses so-called “gag clauses” in form contracts that are designed to stop consumers from providing public feedback that criticizes a company, even when that feedback is an honest reflection of the customer experience. Among other things, this law provides for enforcement by the FTC, and set a deadline of February 12, 2017, for the FTC to begin education and outreach for business to provide them with non-binding best practices for compliance with the law. Please provide an update with respect to the Commission’s activities under this new authority.

Answer. In February 2017, the FTC issued “Consumer Review Fairness Act: What Businesses Need to Know,” a guidance document that informs businesses of the conduct prohibited by the statute and provides information on how to comply with the law. The FTC and states can enforce the law as to contracts in place on or after December 14, 2017.

*Question 7.* This hearing included discussion of the Commission’s role with respect to promoting motor vehicle safety. In a recent panel discussing regulatory and policy issues facing the Commission, you stated your interest in the “safety benefits” of autonomous vehicles and connected cars. Earlier this month, FTC announced a joint...
workshop with the National Highway Traffic Safety Agency (NHTSA), seeking stakeholder input on modern motor vehicle technologies that “promote safety.”

a. Should the Commission defer to the expert Federal agencies, such as NHTSA and the National Transportation Safety Board, on the issue of motor vehicle safety? Answer. The FTC would generally defer to Federal agencies such as NHTSA and the National Transportation Safety Board (NTSB) regarding motor vehicle safety. At the same time, however, the line between issues of safety and non-safety are not necessarily clear. For example, a data security vulnerability may both expose consumers’ personal information, as well as raise vehicle safety concerns. The Commission brings much experience to bear on the former. For example, on the privacy side, several automakers have voluntarily made commitments to adhere to industry privacy principles, and we have unique experience in enforcing self-regulatory codes. On the security side, the Commission has significant expertise in examining software security issues, such as failure to test for the presence of reasonably foreseeable vulnerabilities.

Nonetheless, I share your concern and I am committed to working with other Federal agencies to ensure that the FTC not impose duplicative, overlapping, or conflicting requirements on car companies.

b. Does the Commission have jurisdiction over motor vehicle safety under its unfairness authority, which recognizes that, “unwarranted health and safety risks may also support a finding of unfairness,” or would such actions rely primarily on public policy considerations? Answer. It is possible that, in certain contexts, the FTC’s Section 5 unfairness jurisdiction could apply where a motor vehicle presented unreasonable health and safety risks to consumers. As noted above, I remain committed to working with other Federal agencies to ensure that the FTC not impose duplicative, overlapping, or conflicting requirements on automotive companies.

Question 8. The Senate Commerce Committee has also focused its attention on the issue of the marketing of anti-concussion sports equipment. Does the Commission have sufficient authority under the FTC Act, 15 U.S.C. §§ 41–58, to pursue enforcement actions against companies that engage in false or misleading advertising with respect to these products?

Answer. Section 5 of the FTC Act, 15 U.S.C. § 45(a), prohibits false or misleading advertising, including false or misleading advertising of the anti-concussion benefits of sports equipment. I believe this authority is sufficient to allow the Commission to pursue enforcement actions against companies that engage in false or misleading advertising with respect to these products.

Question 9. In the FTC’s written testimony, the Commission noted scams targeting small commercial trucking businesses wherein scammers impersonate government agencies to solicit payment for Federal motor carrier registration. Small, family-owned trucking companies are an important part of the South Dakota transportation sector. These companies, along with their larger counterparts, must register with the U.S. Department of Transportation (DOT) and re-register periodically. As part of this process, registrant contact information is routinely made available online where it can be accessed by anyone, including scammers. I have heard from South Dakota trucking companies who are concerned about the illegitimate requests and solicitations for unnecessary services they receive. Sometimes, these requests and solicitations come from companies with official-sounding websites such as “DOTcompliance.com” and “ExpressDOTService.com.” Particularly


for smaller companies, it is difficult to discern legitimate requests from illegitimate ones.

a. What steps has the FTC taken to combat this fraudulent behavior? How will the Commission address future incidents?

Answer. The FTC is concerned about this possible misconduct and has been working with the U.S. Department of Transportation (USDOT) to address it. In 2015, USDOT approached the FTC about the deceptive marketing of registration services by companies pretending to be affiliated with government agencies to small, family-owned trucking companies. Since then, the FTC has offered guidance to USDOT on consumer warnings and education measures to combat government-imposter registration solicitations. In addition, USDOT and the FTC worked together to identify and investigate relevant consumer complaints. As a result, this past Fall, the FTC filed an action alleging that several interrelated companies, including DOTAuthority.com, Inc., deceived small commercial trucking businesses into paying them for Federal and state motor carrier registrations by impersonating government transportation agencies. Our complaint alleges that the defendants have taken in more than $17 million from thousands of small businesses by sending misleading robocalls, e-mails, and text messages that create and reinforce the false impression that they are, or are affiliated with, the USDOT, the Unified Carrier Registration System, or another government agency. As alleged in the complaint, the defendants used official-sounding names, official-looking websites, warnings of civil penalties or fines for non-compliance, and threats of imminent law enforcement to trick companies into using their registration services instead of using official government website services. The USDOT submitted two declarations in support of the FTC’s complaint. The court has entered a preliminary injunction against the defendants and the litigation in this case is on-going.

b. To what extent has the FTC worked with DOT to address these scams?

Answer. The FTC is concerned about this possible misconduct and has been working with the USDOT to address it. In 2015, USDOT approached the FTC about the deceptive marketing of registration services by companies pretending to be affiliated with government agencies to small, family-owned trucking companies. Since then, the FTC has offered guidance to USDOT on consumer warnings and education measures to combat government-imposter registration solicitations. In addition, USDOT and the FTC worked together to identify and investigate relevant consumer complaints. As a result, this past Fall, the FTC filed an action alleging that several interrelated companies, including DOTAuthority.com, Inc., deceived small commercial trucking businesses into paying them for Federal and state motor carrier registrations by impersonating government transportation agencies. Our complaint alleges that the defendants have taken in more than $17 million from thousands of small businesses by sending misleading robocalls, e-mails, and text messages that create and reinforce the false impression that they are, or are affiliated with, the USDOT, the Unified Carrier Registration System, or another government agency. As alleged in the complaint, the defendants used official-sounding names, official-looking websites, warnings of civil penalties or fines for non-compliance, and threats of imminent law enforcement to trick companies into using their registration services instead of using official government website services. The USDOT submitted two declarations in support of the FTC’s complaint. The court has entered a preliminary injunction against the defendants and the litigation in this case is on-going.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DEB FISCHER TO HON. MAUREEN K. OHLHAUSEN

Question 1. Acting Chairman Ohlhausen, in both this Congress and the last, I introduced the Spoofing Prevention Act with Ranking Member Nelson and Senators Blunt and Klobuchar. That bill would take steps to close loopholes in the Truth in Caller ID Act so we can better combat spoofing scams against seniors, law enforcement, and members of our military. What do you see as the Federal Trade Commission’s role in eliminating spoofing, and what more needs to be done to fix this problem?

Answer. The FTC uses every tool at its disposal to combat illegal spoofing and fraudulent and deceptive calls to consumers, including aggressive law enforcement, initiatives to spur technological solutions, and robust consumer education. We have brought more than 130 law enforcement actions shutting down operations responsible for billions of illegal calls, as well as numerous enforcement actions targeting fraudulent “impostors.” Many of our law enforcement actions specifically target defendants that engage in illegal spoofing.

In addition to continuous law enforcement in this area, the FTC is committed to working with industry to encourage and facilitate the development and deployment of network-level technological solutions to illegal spoofing. The FTC provided input to support the industry-led Robocall Strike Force, which is working to deliver comprehensive solutions to filter unwanted robocalls and to prevent illegal spoofing. The Robocall Strike Force highlighted two technological solutions that have been underway that will help thwart illegal spoofing: (1) a “do-not originate” list and (2) Caller ID authentication standards. A “do-not originate” list allows the owner of a number to opt out of illegal calls. Caller ID authentication refers to standards to verify and authenticate caller identification for calls carried over an Internet Protocol (IP) network. These standards are known as SHAKEN (Signature-based Handling of Asserted information using toKENs) and STIR (Secure Telephony Identity Revisited). Wide-spread adoption of Caller ID authentication standards would enable...
57

ber to specify that it should only be used to accept incoming calls and never to place outgoing ones. In furtherance of the development of a “do-not-originate” list, the FTC worked with a major carrier and Federal law enforcement partners to help block IRS scam calls that were spoofing well-known IRS telephone numbers.

The FTC also engages with technical experts, academics, and others through industry groups, such as the Messaging, Malware and Mobile Anti-Abuse Working Group (“M3AAWG”) and the Voice and Telephony Abuse Special Interest Group (“VTA SIG”). The FTC serves in a leadership role in VTA SIG, which currently works to support various initiatives that tackle voice spam, including Caller ID authentication standards.

We also arm consumers with the tools and information they need to protect themselves against fraudulent calls that often use spoofed numbers. The FTC provides consumer information in English and Spanish in many forms including print and online articles, fact sheets, blog posts, brochures and videos with tips for avoiding scams and unwanted calls. One of our most popular features is a “Scam Alert” page that is frequently updated with blog posts about new scams. We also remind consumers in our guidance that they need to be wary of scammers using fake Caller ID information.

Question 2. Acting Chairman Ohlhausen, as you may know, there have been many recent reports of travel company booking scams. These involve fraudulent companies imitating the websites of hotels or airlines to attract bookings and trick consumers into paying fees for services they do not receive. I have one such account from a hotel in Kearney, Nebraska, that I entered into the hearing record. Last fall, Senator Klobuchar and I sent you a letter regarding this fraudulent practice. Does the FTC frequently hear about these types of complaints? If so, what would be an appropriate response?

Answer. The FTC has a strong interest in protecting consumer confidence in the online marketplace for travel and other services. The FTC has received complaints about websites that mimic those of well-known travel companies from Members of Congress, industry associations, and consumers. The Consumer Sentinel complaint database, which includes complaints received directly by the FTC as well as complaints contributed by the Better Business Bureau and other agencies, contains approximately 60 complaints since 2012 indicating that consumers had booked a hotel through a third-party site when they thought they were booking directly with a hotel.

In July 2015, the FTC issued consumer education cautioning consumers about third-party websites that may deceptively mimic hotel websites. We also have met with Members of Congress to discuss the issue of deceptive travel sites and have provided technical assistance and comments on proposed legislation. Although the existence and details of investigations are non-public, I can assure you that the FTC staff has taken these complaints seriously and will take law enforcement action if appropriate.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JERRY MORAN TO HON. MAUREEN K. OHLHAUSEN

Question 1. During the hearing, one of the issues raised by both panel members and witnesses was the rise of ransomware, especially targeted at small business owners. One of the devious ways that hackers can gain access to a computer is by baiting Internet users with the prospect of free movies, TV shows or music. Recent studies have found that 1 in 3 so-called pirate websites expose consumers to malware. Given the rise of piracy as a means to bait and infect computers, and increase in ransomware, what is the FTC doing to warn consumers about the connection between piracy and malware?

Answer. I share your concerns about malware on consumers’ computers and the potential harm such malware may cause consumers. Related to the specific practice you have highlighted, last week, the Commission issued a consumer education blog post warning consumers that downloading pirated content is illegal and websites of-
ering such content often hide malware that can bombard them with ads, take over their computers, or steal their personal information.20

Consumer education is a central part of the FTC’s mission. Our outreach includes publications, online resources, workshops, and social media. These outreach efforts cover many topics, including malware, tech support scams, spyware, phishing, peer-to-peer file sharing, and social networking. We work closely with local, state, and Federal Government entities, industry representatives, and consumer groups to maximize the impact of these efforts.

The FTC has many consumer education resources that provide additional information to consumers about dangers associated with malware. For example, the Commission has published blog posts and videos on ransomware21 and identity theft.22 In addition, our Net Cetera publication helps parents, teachers, and other adults talk to children about how to be safe, secure, and responsible online.23 Relevant resources also include education materials relating to individual enforcement actions the Commission has taken. For example, last year the Commission settled an action with ASUSTeK Computer, Inc. in which the Commission alleged that the company’s routers had security bugs that allowed malware to commandeer consumers’ web traffic.24 In connection with this settlement, the Commission published a blog post with tips on router security.25

Question 2. Another theme of the hearing was the economic loss caused by scams. A recent investigation by security company RiskIQ found that hackers are paying pirates operators $70 million a year to infect computers. With the help of the FTC play in warning consumers and encouraging those who facilitate online activity—such as domain sellers, hosting companies, search engine companies and payment processors—in combatting these piracy/malware operators? For example, should the FTC post warnings on their website, produce public service announcements or work with digital platforms to raise awareness and combat this new threat?

Answer. The FTC’s robust law enforcement and consumer education platforms cover many topics, including malware, tech support scams, spyware, phishing, peer-to-peer file sharing, and social networking. We work closely with local, state, and Federal Government entities, industry representatives, and consumer groups to maximize the impact of these efforts. In addition, the Commission has brought several enforcement actions to stop companies from installing malware and other unwanted software on consumers’ computers and devices.26 The Commission will continue to use its investigative, legal, and public outreach tools to protect consumers from unwanted and harmful software. Moreover, the Commission will continue, as it has done in the past, to work with high tech companies, service providers, and industry participants to combat online threats.


Question 3. In the FTC’s prepared testimony, the agency discusses the challenges associated with offshore scammers, including international telemarketing fraud rings. The Committee is also aware that so-called Jamaican lottery scams have proliferated in recent years. One tool available to FTC is the U.S. SAFE WEB Act, which allows the Commission to address consumer protection matters, particularly those with an international dimension, providing for increased cooperation with foreign law enforcement authorities, confidential information sharing and investigative assistance.

a. How has FTC used the SAFE WEB Act in its fight against scams?

Answer. The FTC has used the Act’s powers extensively in cross-border fraud cases and other matters to protect Americans. Between FY 2012 and FY 2016, for example, the FTC used the Act to share information in response to almost 65 requests from foreign agencies, and issued nearly 65 civil investigative demands to aid 28 foreign investigations. These efforts have enabled foreign counterparts to investigate conduct that directly harms American consumers, and, in many instances, also helped to advance FTC investigations. Here are a few examples since Congress reauthorized the Act in 2012:

The FTC used its SAFE WEB powers to work with Canadian law enforcement to stop a telemarketing scam that targeted senior citizens. On the U.S. side, the FTC obtained an order for more than $10 million in consumer redress and the Justice Department charged some of the defendants criminally. On the Canadian side, the Royal Canadian Mounted Police (RCMP) brought its own case, arresting the Canadian-based defendants and seizing evidence.

The FTC used its SAFE WEB powers to obtain evidence for the Toronto Police Service’s investigation of a sham business that scammed $93 million from consumers by purporting to sell banner ads for websites. The scheme had thousands of victims worldwide, including in the United States. Canadian law enforcement broke up the scam and arrested two of its leaders.

The FTC used its SAFE WEB authority in another telemarketing scam to repatriate, with Justice Department help, nearly $2 million of the defendant’s assets from Canadian bank accounts frozen by the RCMP; the FTC has now sent redress checks to 1,630 victims totaling $1.8 million.

The FTC has used SAFE WEB in a number of business directory scams that prey on small businesses, non-profits, and churches to share evidence with counterparts in Canada and other jurisdictions. This has led to several FTC judgments and law enforcement actions in Canada.

SAFE WEB also allowed the FTC to exchange information with Canadian law enforcement about a company that put unauthorized charges on consumers’ phone bills using phony virus-scan scareware and led to law enforcement actions involving that conduct on both sides of the border.

Apart from scams, the Act also supports FTC enforcement of the EU–U.S. Privacy Shield Framework, which enables transatlantic data flows for many U.S. companies. The FTC’s SAFE WEB powers provide for stronger cooperation with European data protection authorities on investigations and enforcement against possible Privacy Shield violations, a point cited in the European Commission’s Privacy Shield adequacy decision.


b. This legislation is scheduled to sunset in 2020. Do you support its reauthorization? Will you commit to provide technical assistance to the Committee, including any modifications to improve the FTC’s ability to go after international scammers?

Answer. I strongly support SAFE WEB reauthorization and commit to providing technical assistance to the Committee for that process. FTC staff worked closely with the Committee to develop the original legislation passed in 2006, and to support reauthorization in 2012. We would be pleased to work with the Committee to continue strengthening our ability to go after international scammers. We in particular suggest repealing the sunset provision entirely: greater certainty for the agency and our international partners about the FTC’s enforcement tools going forward improves our ability to develop enduring cooperation agreements and enforcement projects with foreign counterparts. Congress granted the Securities and Exchange Commission and the Commodities and Futures Trading Commission similar enforcement powers over 25 years ago, without a sunset provision. Their positive enforcement cooperation experience, and the FTC’s successful experience with SAFE WEB over the past decade, confirms the value of this legislation to our enforcement mission.

Question 4. The FTC’s prepared statement for the hearing raised concerns with the controversial “common carrier” exception from Title II of the Communications Act and its impact on the FTC’s efforts to protect consumers from unfair or deceptive acts or practices. Could you please elaborate on how this provision is harming the FTC’s mission? Additionally, how did the Court of Appeals for the Ninth Circuit’s recent decision holding that the “common carrier” exception is “status based” affect the FTC’s ability to protect consumers?

Answer. Section 5 of the FTC Act prohibits “unfair or deceptive acts or practices” in or affecting commerce and directs the FTC to prevent such conduct. 15 U.S.C. § 45(a). Section 5, however, excepts from FTC enforcement authority “common carriers subject to the Acts to regulate commerce.”34 The FTC has long interpreted this exception to be “activity based”—that a company that engaged in both common carriage and non-common carriage activities would still be within the FTC’s enforcement authority with regards to the non-common carriage activities. Even with this limiting interpretation, however, the FTC, on a bipartisan basis, has for many years called for repeal of the exception as outdated, unnecessary, and a hindrance to consumer protection efforts.

The common carrier exception poses several obstacles to the FTC effectively carrying out its consumer protection mission. For example, some companies have objected to an FTC enforcement action on the basis of the common carrier exception.35 Even when such objections are meritless, the FTC is forced to litigate this issue in the court systems, which diverts FTC resources from other consumer protection efforts and can delay redress to fraud victims.

Furthermore, consumers should be protected from unfair or deceptive acts or practices in the entire marketplace. But the common carrier exception effectively excludes a subset of consumers’ activities in the marketplace from this protection. This problem has been put into sharper focus as a result of the Federal Communications Commission’s action in 2015 reclassifying the provision of broadband Internet service as a common carrier activity. Prior to this action, provision of Internet services was considered a non-common carrier activity and the FTC was able to enforce consumer protection laws against Internet service providers, even in the early days of the internet. For example, in 1998, the FTC brought an action against AOL and other ISPs for allegedly deceptive “free” trial periods.36 However, the FCC’s reclassification created an enforcement gap in which the FTC may now be unable to protect consumers from unfair or deceptive practices by ISPs.

The Ninth Circuit’s recent decision has further exacerbated the problem by applying a “status based” interpretation to the common carrier exception. Under this interpretation, if a company has the status of common carrier, all of its activities, even those not related to common carriage, could be immune from FTC enforcement authority. This would further weaken consumer protection efforts, including in areas in which the FTC has taken significant law enforcement actions in the past. For example, the agency sued AT&T and T-Mobile in 2013 for placing unauthorized

Footnotes:
34 In 1914 when the FTC Act was passed, Section 4 of the Act defined “Acts to regulate commerce” as the Interstate Commerce Act; Congress later added the Communications Act. See 15 U.S.C. § 44.
35 See, e.g., FTC v. Verity Int’l, Ltd., 443 F.3d 48 (2d Cir. 2006).
charges for purported third-party services on consumers' mobile phone bills.37 Those and similar cases have recovered hundreds of millions of dollars for injured consumers. The Ninth Circuit decision calls into question the agency’s ability to take similar actions in the future.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. DEAN HELLER TO HON. MAUREEN K. OHLHAUSEN

Question. Last Congress, Microsoft came before the Senate Aging Committee and told us about partnerships they had with states to combat tech scams. For Nevadans, consumer protection is a top issue, especially because of the impact that scams can have on an individual's finances or even their privacy. Are there any FTC initiatives in coordination with State Attorneys General that are models for protecting consumers from scams? Answer. The Commission has robust, collaborative relationships with state law enforcers, including through the National Association of Attorneys General. The FTC has collaborated with its state partners on dozens of joint enforcement actions, including investigations and enforcement actions concerning tech support scams, robocalls, debt collection practices, among other deceptive and unfair practices. The FTC also leads law enforcement “sweeps”—coordinated, simultaneous law enforcement actions—in conjunction with state and local partners. To supplement its law enforcement efforts, the FTC and its state partners also co-host consumer protection conferences and workshops designed to protect consumers from fraud and provide guidance on how to identify and avoid scams.43


43 See, e.g., Events Calendar, FTC & NASCO Host a Conference Exploring Consumer Protection Issues and Charitable Solicitations (Mar. 21, 2017), available at www.ftc.gov/news-events/events-calendar/2017/03/give-take-consumers-contributions-charity; Events Calendar, Working...
Response to Written Questions Submitted by Hon. Todd Young to Hon. Maureen K. Ohlhausen

Question 1. Acting Chairman Ohlhausen and Commissioner McSweeny, has the FTC focused on the issue of travel booking scams beyond issuing consumer alerts?
Answer. As you note, in July 2015, the FTC issued consumer education cautioning consumers about third-party websites that may deceptively mimic hotel websites. In addition, we have met with Members of Congress to discuss the issue of deceptive travel sites and have proposed technical assistance and comments on proposed legislation. Because the existence and details of investigations are non-public, we cannot comment on any specific matters. However, the FTC will take law enforcement action in appropriate cases.

Question 2. Acting Chairman Ohlhausen and Commissioner McSweeny, what plans does the FTC have to notify and coordinate with State Attorney Generals prior to peak travel season this year, including summer, Thanksgiving, and the Christmas holidays?
Answer. The FTC has worked closely with the State Attorneys General on many issues, including most recently during National Consumer Protection week. The FTC will explore whether there are opportunities to coordinate with the states to protect consumers from scams that affect them during these peak travel periods.

Question 3. Acting Chairman Ohlhausen: In your testimony, you noted that military consumers are often attractive targets of fraudsters in part because they receive a regular paycheck and move relatively frequently. As a former Marine myself, I can imagine there is also a certain amount of embarrassment among our service men and women when they are taken advantage of and therefore there might be even be lower reporting from victims in this community.
Answer. I agree. In addition to the points you raise, some fraudsters have customized their scams to play on the particular fears of military consumers, such as threatening action under the Uniform Code of Military Justice, which may also lead to under-reporting by this community.

Question 4. Acting Chairman Ohlhausen, in looking at this particular community, do you need additional authority from Congress to work with our service branches to protect military members from potential scams?
Answer. At this time, the Commission has not asked for any specific additional legislation for protecting military members from potential scams. We would, however, be happy to review and provide assistance on any specific piece of proposed legislation.

We have used our existing tools, including the FTC Act, the Fair Debt Collection Practices Act, the Telemarketing Sales Rule, and the Mortgage Assistance Relief Services Rule, to protect military consumers, and we will continue to do so. For example, earlier this year, the Commission announced settlements with two online high schools that claimed their diplomas could be used to join the military and that their programs conformed to the Department of Defense’s SCORM standards for the training of military and civilian personnel. The FTC alleged that these diploma mills violated the FTC Act by failing to provide the promised valid high school equivalency degrees. As part of our investigation, we worked with DoD to provide evidence that the program was not SCORM-conformant.

In other instances, the FTC has brought actions against scammers that target the general population but tailor their practices to deceive military consumers. In one recent case against a fraudulent debt collector, we talked to a consumer whose family was harassed while he was on active duty, and who was threatened with action under the Uniform Code of Military Justice, all about a debt he did not actually owe. We have used our existing tools, including the FTC Act, the Fair Debt Collection Practices Act, the Telemarketing Sales Rule, and the Mortgage Assistance Relief Services Rule, to protect military consumers, and we will continue to do so. For example, earlier this year, the Commission announced settlements with two online high schools that claimed their diplomas could be used to join the military and that their programs conformed to the Department of Defense’s SCORM standards for the training of military and civilian personnel. The FTC alleged that these diploma mills violated the FTC Act by failing to provide the promised valid high school equivalency degrees. As part of our investigation, we worked with DoD to provide evidence that the program was not SCORM-conformant.

In other instances, the FTC has brought actions against scammers that target the general population but tailor their practices to deceive military consumers. In one recent case against a fraudulent debt collector, we talked to a consumer whose family was harassed while he was on active duty, and who was threatened with action under the Uniform Code of Military Justice, all about a debt he did not actually owe. We have used our existing tools, including the FTC Act, the Fair Debt Collection Practices Act, the Telemarketing Sales Rule, and the Mortgage Assistance Relief Services Rule, to protect military consumers, and we will continue to do so. For example, earlier this year, the Commission announced settlements with two online high schools that claimed their diplomas could be used to join the military and that their programs conformed to the Department of Defense’s SCORM standards for the training of military and civilian personnel. The FTC alleged that these diploma mills violated the FTC Act by failing to provide the promised valid high school equivalency degrees. As part of our investigation, we worked with DoD to provide evidence that the program was not SCORM-conformant.

In other instances, the FTC has brought actions against scammers that target the general population but tailor their practices to deceive military consumers. In one recent case against a fraudulent debt collector, we talked to a consumer whose family was harassed while he was on active duty, and who was threatened with action under the Uniform Code of Military Justice, all about a debt he did not actually owe.
owe.49 The FTC was able to obtain a court order banning these collectors from the debt collection industry and imposing monetary judgments against them. In another case, the FTC brought an action alleging that a sham non-profit claimed it would provide legal representation to struggling homeowners trying to avoid foreclosure but failed to provide the promised services.50 One consumer we talked to was an elderly veteran amputee who had paid almost $10,000 to the scammers to obtain a mortgage loan modification and received nothing of value in return. The FTC obtained an order banning the scammers from the mortgage and debt relief industries and returned approximately $3 million to alleged victims of the scam.

**Question 5.** Acting Chairman Ohlhausen, what specific efforts has the FTC undertaken with our service branches to help protect our service men and women?

**Answer.** Protecting military consumers through law enforcement and education is a top priority of the Commission, and we work closely with military partners to help the military community avoid frauds. Military Consumer is the FTC’s longstanding campaign to reach service members and their families. The FTC website I mentioned in my testimony, Military.Consumer.gov, is a joint initiative with Department of Defense, the CFPB’s Office of Servicemember Affairs, Military Saves, FINRA Investor Education Foundation, the National Military Family Association and other partners to empower active duty and retired servicemembers, military families, veterans, and civilians in the military community. The site’s Military Consumer Toolkit offers free materials on topics that allow personal financial managers, counselors, command, and others in the military community to share practical financial readiness tips.

While Military Consumer is a year-round campaign, each July the FTC hosts the Month of the Military Consumer with the Department of Defense to bring additional focus to consumer issues affecting servicemembers and military families. This year, the FTC will be hosting a free workshop on July 19, 2017, to examine financial issues and scams that can affect military consumers, including active duty service members in all branches and veterans. Topics of discussion at the daylong event will include auto purchasing, financing, and leasing; student and other lending; information security issues; financial literacy and capability, including identity theft; and avoiding scams.51 We are working closely with our military partners in planning an event that will bring together all service branches, military consumer advocates, military legal services, government representatives, and industry representatives.

The agency regularly disseminates short tips through social media and hosts periodic Twitter chats with federal, state, and military partners. In addition to our online materials, the FTC also has presented webinars and made presentations for personal financial managers in conjunction with the Army, the Navy, the Department of Veterans Affairs, Military One Source, the Military Family Learning Network (and USDA Cooperative Extension), and military contractors serving as counselors to military families.

The Commission will continue to work with our military partners to protect our service men and women from unfair and deceptive acts and practices.

**RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. BILL NELSON TO HON. MAUREEN K. OHLHAUSEN**

**Question.** The FTC already operates on a tight budget. It is a small agency with a huge mandate: to police the American economy and enforce against “unfair or deceptive acts or practices.” The Trump Administration has proposed irresponsible cuts to virtually every aspect of the government that helps the average American. While we have yet to see a specific budget proposal for the FTC, the “skinny” budget did reference a vague 9.8 percent cut to “other agencies” that were not specifically mentioned. It seems safe to say that funding cuts may well be coming to the FTC. How would a possible budget cut—say, along the lines of a 9.8 percent cut—affect the FTC’s ability to protect American consumers from scams and fraud?
Answer. We are currently working with OMB to determine what the President's 2018 budget will recommend for the Commission and we are optimistic that it will not propose a significant cut for the agency. However, if the FTC faced a significant budgetary cut, we would strive to minimize its effect on the Commission's ability to enforce consumer protection and competition laws, though it would likely have some impact.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. RICHARD BLUMENTHAL TO HON. MAUREEN K. OHLHAUSEN

Question 1. In March, the DOJ indicted four individuals, including two Russian spies, for hacking into Yahoo’s systems in 2014 and obtaining access to at least 500 million Yahoo accounts. According to the indictment, defendants spied on U.S. government officials and private-sector employees of financial companies, among others. One defendant also exploited the data for financial gain. He searched user e-mail accounts for gift card numbers, redirected Yahoo search traffic so he could make commissions, and stole the contacts of at least 30 million Yahoo accounts to conduct a spam marketing scheme. What are the chances of the United States taking these Russian spies into custody for their crimes?

Answer. The FTC does not have criminal law enforcement authority, but it works closely with its criminal and foreign law enforcement partners to achieve a broader impact and further its mission of protecting consumers. For example, as noted during the March 21, 2017, hearing before this Subcommittee, the Commission created the Criminal Liaison Unit in 2003, and FTC prosecution referrals have led to hundreds of fraudsters facing criminal charges and prison time.

While the FTC encourages criminal authorities to pursue hackers, we also believe it is important for companies to shore up the security of their systems, so that they can help protect against unauthorized access to, and misuse of, consumer data. Unfortunately, reports of data breaches like the one you cite affect millions of Americans. The Commission is deeply concerned about the risk of fraud, identity theft, and other harm that consumers face as a result of such breaches, which is why promoting data security has long been, and will continue to be, a priority.

The Commission enforces several civil statutes and rules that impose security obligations upon businesses that collect and maintain consumer data. The Commission’s Safeguards Rule, which implements the Gramm-Leach-Bliley Act, for example, provides data security requirements for financial institutions within the Commission’s jurisdiction. The Fair Credit Reporting Act (“FCRA”) requires consumer reporting agencies to use reasonable procedures to ensure that the entities to which they disclose sensitive consumer information have a permissible purpose for receiving that information, and imposes safe disposal obligations on entities that maintain consumer report information. The Children’s Online Privacy Protection Act (“COPPA”) requires reasonable security for children’s information collected online. In addition, the Commission enforces Section 5 of the FTC Act, which prohibits unfair or deceptive acts or practices, such as businesses making false or misleading claims about their data security procedures, or failing to employ reasonable security measures and, as a result, causing or likely causing substantial consumer injury.

Since 2001, the Commission has used its authority under these laws to take enforcement action and obtain settlements in approximately 60 cases against businesses that it charged with failing to provide reasonable and appropriate protections for consumers’ personal information.

In addition to bringing enforcement actions, the Commission engages in significant educational efforts discussed in more detail below. In all of its efforts, the Commission looks forward to continued cooperation and collaboration with its law enforcement partners, and with private industry, to protect the security of consumers’ data.

Id. at § 1681w. The FTC’s implementing rule is at 16 C.F.R. Part 682.
15 U.S.C. § 45(a). If a company makes materially misleading statements or omissions about a matter, including data security, and such statements or omissions are likely to mislead reasonable consumers, they can be found to be deceptive in violation of Section 5. Further, if a company’s data security practices cause or are likely to cause substantial injury to consumers that is neither reasonably avoidable by consumers nor outweighed by countervailing benefits to consumers or to competition, those practices can be found to be unfair and violate Section 5.
Question 2. So, despite our country and the Department of Justice’s best efforts, our country remains vulnerable to outside threats seeking to infiltrate our systems and prey on our consumers. The New York Times has also reported that despite DOJ’s indictment against the individuals responsible for these attacks, one billion Yahoo accounts—stolen in another attack on the company a year earlier—continue to be found for sale on underground hacker forums as recently as last Friday, for $200K. This is a stark reminder that while Federal prosecutors are taking steps they can to hold the criminals and perpetrators accountable, private consumer information is still available and vulnerable for abuse. Do you think Yahoo has implemented reasonable security standards to protect its customers?

Answer. The Commission can only determine whether a company’s practices are reasonable after conducting an investigation. Because Yahoo has made our investigation public in a filing with the Securities and Exchange Commission, I can confirm that we are investigating the company. But Commission rules prevent me from making any further comments about the details of our investigation.

More generally, through its enforcement actions and education materials,7 the Commission has publicly provided the core principles that it applies when looking at a company’s data security practices. For example, the Commission does not require perfect data security and the mere fact that a breach occurred does not mean that a company has violated the law. Rather, a company’s security must be reasonable under the circumstances. There is no one-size-fits-all approach to what constitutes reasonable data security and what is reasonable will vary, depending on the size and complexity of a company’s operations, the amount and sensitivity of the data it collects, and the availability of low-cost tools to mitigate threats. Thus, a large company collecting vast amounts of sensitive data will need to have different measures in place than a company collecting small amounts of non-sensitive data. Reasonable security should also include a continuous process of assessing and addressing risks.

The FTC will continue to apply these principles as it uses its civil law enforcement authority to promote data security in the private sector.

Question 3. According to a recent study, one out of three content theft sites expose consumers to malware, leading to compromised bank accounts, identity theft, and “ransomware” that locks a consumer out of their data until they pay the criminals the required ransom. This study showed that 45 percent of malware was delivered by “drive-by-downloads,” which invisibly download to a user’s computer without requiring them to click on a link. What is the FTC doing to inform and educate consumers about the link between content theft sites and malware?

Answer. I share your concerns about malware on consumers’ computers and the potential harm such malware may cause consumers. Related to the specific practice you have highlighted, last week the Commission issued a consumer education blog post warning consumers that downloading pirated content is illegal and cautioning that websites offering such content often hide malware that can bombard them with ads, take over their computers, or steal their personal information.8

Consumer education is a central part of the FTC’s mission. Our outreach includes publications, online resources, workshops, and social media. These outreach efforts cover many topics, including malware, tech support scams, spyware, phishing, peer-to-peer file sharing, and social networking. We work closely with local, state, and Federal Government entities, industry representatives, and consumer groups to maximize the impact of these efforts.

The FTC has many consumer education resources that provide additional information to consumers about dangers associated with malware. For example, the Commission has published blog posts and videos on ransomware9 and identity

---

theft. In addition, our Net Cetera publication helps parents, teachers, and other adults talk to children about how to be safe, secure, and responsible online.

Relevant resources also include education materials relating to individual enforcement actions the Commission has taken. For example, last year the Commission settled an action with ASUSTeK Computer, Inc. in which the Commission alleged that the company’s routers had security bugs that allowed malware to commandeer consumers’ web traffic. In connection with this settlement, the Commission published a blog post with tips on router security.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. AMY KLOBUCHAR TO HON. MAUREEN K. OHLHAUSEN

Question. Malware that gives fraudsters access to consumers’ computers can be a powerful tool for scams. In one model, websites that offer pirated content, bogus coupons, or fake products are paid to infect computers with malware. Sometimes just visiting one of these websites—without even clicking on anything—can be enough to infect your computer with malware. Scammers can then use the infected computers to access financial information, launch cyberattacks, or even take over the computer’s camera.

Chairman Ohlhausen, what is the FTC doing to educate consumers about the danger of websites designed to infect their computers with malware?

Answer. I share your concerns about malware on consumers’ computers and the potential harm such malware may cause consumers. Related to the specific practice you have highlighted, last week, the Commission issued a consumer education blog post warning consumers that downloading pirated content is illegal and websites offering such content often hide malware that can bombard them with ads, take over their computers, or steal their personal information.

Consumer education is a central part of the FTC’s mission. Our outreach includes publications, online resources, workshops, and social media. These outreach efforts cover many topics, including malware, tech support scams, spyware, phishing, peer-to-peer file sharing, and social networking. We work closely with local, state, and Federal Government entities, industry representatives, and consumer groups to maximize the impact of these efforts.

The FTC has many consumer education resources that provide additional information to consumers about dangers associated with malware. For example, the Commission has published blog posts and videos on ransomware and identity theft. In addition, our Net Cetera publication helps parents, teachers, and other adults talk to children about how to be safe, secure, and responsible online.

Relevant resources also include education materials relating to individual enforcement actions the Commission has taken. For example, last year the Commission settled an action with ASUSTeK Computer, Inc. in which the Commission alleged that the company’s routers had security bugs that allowed malware to commandeer consumers’ web traffic. In connection with this settlement, the Commission published a blog post with tips on router security.

---

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JERRY MORAN TO HON. TERRELL MCSWEENY

Question 1. During the hearing, one of the issues raised by both panel members and witnesses was the rise of ransomware, especially targeted at small business owners. One of the devious ways that hackers can gain access to a computer is by baiting Internet users with the prospect of free movies, TV shows or music. Recent studies have found that 1 in 3 so-called pirate websites expose consumers to malware. Given the rise of piracy as a means to bait and infect computers, and increase in ransomware, what is the FTC doing to warn consumers about the connection between piracy and malware?

Answer. The Commission recently published a blog post on the FTC’s website entitled “Free movies, costly malware” to educate consumers about the possibility that pirate websites will infect their computers and devices with malware if they download copyrighted content.1 We also have posted the blog to military.consumer.gov. The FTC will continue to warn consumers about the risks associated with downloading content from pirate websites, as appropriate. I am very concerned about ransomware and fear the danger to businesses and consumers will only grow. This is an issue that the FTC, Congress, and law enforcement at every level must collaborate on to provide better solutions to American consumers and businesses.

Question 2. Another theme of the hearing was the economic loss caused by scams. A recent investigation by security company RiskIQ found that hackers are paying pirate website operators $70 million a year to infect computers. What role should the FTC play in warning consumers and encouraging those who facilitate online activity—such as domain sellers, hosting companies, search engine companies and payment processors—in combatting these piracy/malware operators? For example, should the FTC post warnings on their website, produce public service announcements or work with digital platforms to raise awareness and combat this new threat?

Answer. The FTC has a robust law enforcement and consumer education platform designed to combat online threats, such as the unwanted installation of malware and other software. For instance, last fall, the FTC held a workshop with numerous industry participants to educate consumers about how to avoid—and respond to—ransomware.2 And, as noted in response to the previous question, the FTC recently published a blog post on its website entitled “Free movies, costly malware” to educate consumers about the possibility that pirate websites will infect their computers and devices with malware if they download copyrighted content.3 The FTC also produced a consumer education video about how to avoid, detect, and remove malware.4

In addition, the Commission has brought several enforcement actions to stop companies from installing malware and other unwanted software on consumers’ computers and devices.5 The Commission will continue to use its investigative, legal, and public outreach tools to protect consumers from unwanted and harmful software. Moreover, the Commission will continue, as it has done in the past, to work with high tech companies, service providers, and industry participants to combat online threats.

Question 3. In the FTC’s prepared testimony, the agency discusses the challenges associated with offshore scammers, including international telemarketing fraud rings. The Committee is also aware that so-called Jamaican lottery scams have proliferated in recent years. One tool available to FTC is the U.S. SAFE WEB Act,

---

which allows the Commission to address consumer protection matters, particularly those with an international dimension, providing for increased cooperation with foreign law enforcement authorities, confidential information sharing and investigative assistance.

a. How has FTC used the SAFE WEB Act in its fight against scams?

Answer. The FTC has used the Act’s powers extensively in cross-border fraud cases and other matters to protect Americans from cross-border fraud. Between FY 2012 and FY 2016, for example, the FTC used the Act to share information in response to almost 65 requests from foreign agencies, and issued nearly 65 civil investigative demands to aid 28 foreign investigations. These efforts have enabled foreign counterparts to investigate conduct that directly harms American consumers, and also helped to advance FTC investigations in many instances. Here are a few examples since Congress reauthorized the Act in 2012:

The FTC used its SAFE WEB powers to work with Canadian law enforcement to stop a telemarketing scam that targeted senior citizens. On the U.S. side, the FTC obtained an order for more than $10 million in consumer redress and the Justice Department charged some of the defendants criminally. On the Canadian side, the Royal Canadian Mounted Police (RCMP) brought its own case, arresting the Canadian-based defendants and seizing evidence. (FTC v. First Consumers)6

The FTC used its SAFE WEB powers to obtain evidence for the Toronto Police Service’s investigation of a sham business that scammed $93 million from consumers by purporting to sell banner ads for websites. The scheme had thousands of victims worldwide, including in the United States. Canadian law enforcement broke up the scam and arrested two of its leaders. (RCMP action against Banners’ Broker)7

The agency used its SAFE WEB authority in another telemarketing scam to repatriate, with Justice Department help, nearly $2 million of the defendant’s assets from Canadian bank accounts frozen by the RCMP; the FTC has now sent redress checks to 1,630 victims totaling $1.8 million. (FTC v. Expense Management of America)8

The FTC has used SAFE WEB in a number of business directory scams that prey on small businesses, non-profits and churches to share evidence with counterparts in Canada and other jurisdictions. This has led to several FTC judgments and law enforcement actions in Canada. (E.g., FTC v. Medical Yellow Directories, FTC v. Modern Technology)9

SAFE WEB also allowed the FTC to exchange information with Canadian law enforcement about a company that put unauthorized charges on consumers’ phone bills using phony virus-scan scareware and led to law enforcement actions involving that conduct on both sides of the border. (FTC v. Jesta Mobile Media, Competition Bureau Canada action against Telus)10

Apart from scams, the Act also supports FTC enforcement of the EU-U.S. Privacy Shield Framework, which enables transatlantic data flows for many U.S. companies. The FTC’s SAFE WEB powers provide for stronger cooperation with European data protection authorities on investigations and enforcement against possible Privacy Shield violations, a point cited in the European Commission’s Privacy Shield adequacy decision.

---

b. This legislation is scheduled to sunset in 2020. Do you support its reauthorization? Will you commit to provide technical assistance to the Committee, including any modifications to improve the FTC’s ability to go after international scammers?

Answer. I strongly support SAFE WEB reauthorization and commit to providing technical assistance to the Committee for that process. FTC staff worked closely with the Committee to develop the original legislation passed in 2006, and to support reauthorization in 2012. We would be pleased to work with the Committee to continue strengthening our ability to go after international scammers. We in particular suggest repealing the sunset provision entirely: greater certainty for the agency and our international partners about the FTC’s enforcement tools going forward improves our ability to develop enduring cooperation agreements and enforcement projects with foreign counterparts. Congress granted the SEC and the CFTC similar enforcement powers over 25 years ago, without a sunset provision. Their positive enforcement cooperation experience, and the FTC’s successful experience with SAFE WEB over the past decade, confirms the value of this legislation to our enforcement mission.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. DEAN HELLER TO HON. TERRELL MCSWEENEY

Question. Last Congress, Microsoft came before the Senate Aging Committee and told us about partnerships they had with states to combat tech scams. For Nevadans, consumer protection is a top issue, especially because of the impact that scams can have on an individual’s finances or even their privacy. Are there any FTC initiatives in coordination with State Attorneys General that are models for protecting consumers from scams?

Answer. The Commission has robust, collaborative relationships with state law enforcers, including through the National Association of Attorneys General. The FTC’s collaboration with its state partners takes many forms, including sharing information and targets, assisting with investigations, and working collaboratively on long-term policy initiatives.

Over the last two years, the FTC has collaborated with its state partners on dozens of investigations and numerous joint enforcement actions, including investigations and enforcement actions concerning tech support scams,11 robocalls,12 charity scams,13 and debt collection practices,14 among other deceptive and unfair practices. The FTC also leads law enforcement “sweeps”—coordinated, simultaneous law enforcement actions—in conjunction with state and local partners.15 To supplement its


law enforcement efforts, the FTC and its state partners also co-host consumer protection conferences and workshops designed to protect consumers from fraud and provide guidance on how to identify and avoid scams.16

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TODD YOUNG TO HON. TERRELL MCSWEENY

Question 1. Commissioner McSweeny, has the FTC focused on the issue of travel booking scams beyond issuing consumer alerts?

Answer. As you note, in July 2015, the FTC issued consumer education cautioning consumers about third-party websites that may deceptively mimic hotel websites. In addition, we have met with members of Congress to discuss the issue of deceptive travel sites and have proposed technical assistance and comments on proposed legislation. Because the existence and details of investigations are non-public, we cannot comment on any specific matters. However, the FTC will take law enforcement action in appropriate cases.

Question 2. Commissioner McSweeny, what plans does the FTC have to notify and coordinate with State Attorney Generals prior to peak travel season this year, including summer, Thanksgiving, and the Christmas holidays?

Answer. The FTC has worked closely with the State Attorneys General on many issues, including most recently during National Consumer Protection week. The FTC will explore whether there are opportunities to coordinate with them to protect consumers from scams that affect them during these peak travel periods.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. BILL NELSON TO HON. TERRELL MCSWEENY

Question. The FTC already operates on a tight budget. It is a small agency with a huge mandate: to police the American economy and enforce against "unfair or deceptive acts or practices." The Trump Administration has proposed irresponsible cuts to virtually every aspect of the government that helps the average American. While we have yet to see a specific budget proposal for the FTC, the "skinny" budget did reference a vague 9.8 percent cut to "other agencies" that were not specifically mentioned. It seems safe to say that funding cuts may well be coming to the FTC. How would a possible budget cut—say, along the lines of a 9.8 percent cut—affect the FTC’s ability to protect American consumers from scams and fraud?

Answer. The FTC is still working with OMB to determine what the President’s budget will recommend for us in 2018. We are optimistic that the budget will not propose a significant cut for the Commission. To respond to your question, however, were the FTC’s appropriation to be cut by 9.8 percent, this could significantly affect the Commission’s ability to enforce consumer protection and competition laws.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. RICHARD BLUMENTHAL TO HON. TERRELL MCSWEENY

Question 1. Last year, the FTC successfully finalized settlements with two remaining sham cancer charities—out of four—that had siphoned more than $187 million from donors. This marked the largest joint enforcement effort ever by the FTC and state charity regulators. These fraudulent charities—named “Cancer Fund of America” and “Cancer Support Services,” claimed to help cancer patients. However, the overwhelming majority of donations were lavishly spent on the fake charities’ operators and their families and friends, as well as on fundraisers who shamelessly spent donations on cars, trips, luxury cruises, college tuition, gym memberships, Jet Ski outings, sporting event and concert tickets, and dating site mem-

bersonships. According to the 2015 FTC complaint, this misappropriation of consumer donations dated back to 2008. How were these sham charities able to rob donors of so much money and for so long?

Answer. As you note, in March 2016, the FTC, all 50 states and the District of Columbia resolved litigation against the remaining defendants in Cancer Fund of America, resulting in, among other things, a dissolution of the sham charities and a ban on the companies president’s ability to profit from any charity fundraising in the future.¹ These sham outfits were quite adept at masking their charade. For example, they hid their wrongdoing by manipulating their financial reporting and using deceptive and invalid accounting techniques to claim huge donations of gifts-in-kind. This allowed them to inflate their reported revenue and program spending by $223 million, which allowed the organizations to appear both larger and more efficient with donors’ money than they really were. It was not obvious from their public financial reports to the IRS or the states that less than 2 percent of donated cash was being spent on any program services (collectively).

In addition, charity fraud is easy to miss and underreported. The average donation to the sham cancer charities was less than $30, and the vast majority of those donations were made in response to telephone solicitations. Consumers who gave in response to the promise that their donation would help cancer patients never knew that their money did not go to that cause—and thus did not complain. Further, based on our experience, we believe that few donors take the time to research a $20 to $30 donation before giving, and in this case, the sham charities’ false reporting would have hidden any red flags from even the most diligent consumers.

Question 1. In what way has the nonprofit exemption in the FTC Act hamstrung the Commission's ability to act swiftly to prevent or stop illegal conduct in the nonprofit sector?

Answer. Since nonprofit entities fall outside of the FTC’s jurisdiction, we cannot take action when a “legitimate” charity crosses the line and engages in deceptive or unfair acts and practices. Instead, we can only reach illegal conduct if we can establish that the charity is a “sham.” A sham charity is one that operates primarily to profit individuals and private interests over its beneficiaries. Proving that a charity is a sham requires significant probing into the internal operations of the organization, including detailed review and analysis of bank records and other financial records, board meeting minutes, and employment practices among other things. Not surprisingly, making this threshold proof is difficult, and in some cases impossible—leaving some charitable entities that engage in deceptive practices beyond our reach.

Question 2. In what way has the nonprofit exemption in the FTC Act hamstrung the Commission’s ability to act swiftly to prevent or stop illegal conduct in the nonprofit sector?

Answer. Since nonprofit entities fall outside of the FTC’s jurisdiction, we cannot take action when a “legitimate” charity crosses the line and engages in deceptive or unfair acts and practices. Instead, we can only reach illegal conduct if we can establish that the charity is a “sham.” A sham charity is one that operates primarily to profit individuals and private interests over its beneficiaries. Proving that a charity is a sham requires significant probing into the internal operations of the organization, including detailed review and analysis of bank records and other financial records, board meeting minutes, and employment practices among other things. Not surprisingly, making this threshold proof is difficult, and in some cases impossible—leaving some charitable entities that engage in deceptive practices beyond our reach.

Question 3. According to a recent study, one out of three content theft sites expose consumers to malware, leading to compromised bank accounts, identity theft, and “ransomware” that locks a consumer out of their data until they pay the criminals the required ransom. This study showed that 45 percent of malware was delivered by “drive-by-downloads,” which invisibly download to a user’s computer without requiring them to click on a link. What is the FTC doing to inform and educate consumers about the link between content theft sites and malware?

Answer. I share your concerns about malware on consumers’ computers, which can lead to anything from nuisance adware that delivers pop-up ads, to software that causes sluggish computer performance, to keyloggers that capture sensitive information. The Commission will soon issue a blog post warning consumers that websites offering free content often hide malware that can bombard them with ads, take over their computers, or steal their personal information. More generally, the FTC uses a variety of methods to provide consumers with information about the privacy and security implications of new and existing technologies, and how to avoid and detect malicious software.

Our outreach includes publications, online resources, workshops, and social media. Among the many topics we cover are malware, tech support scams, spyware, phishing, peer-to-peer file sharing, and social networking. Among the resources we have that may be useful are a blog post and video describing the nature of the ransomware threat, how to defend against ransomware, and essential steps for victims to take.²

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. JOHN THUNE TO HON. MIKE DEWINE

Question. One of the biggest challenges Federal agencies face is to fulfil their missions while making the most of limited resources. This is certainly true of the FTC and its mandate to protect American consumers. Can you share your views on how the FTC uses its relationships with state and local law enforcement both to provide assistance and to bolster its own consumer protection efforts? Is there a good level of coordination, or would you like to see more from FTC?

Answer. The relationship between my office and the Federal Trade Commission’s Cleveland Regional Office has historically been very strong. Our Assistant Attorneys General are in fairly regular communication with the FTC’s staff and have participated in a number of coordinated sweeps. That being said, there is always room for improvement.

Like many Federal agencies, the FTC is hesitant to share investigative work product with state and local officials. Some of this may be by necessity. However, by promoting more open lines of communication and sharing of information, we could avoid duplicative work and, perhaps, end up with better results for consumers.

In certain cases, the FTC also keeps attorneys general informed of Federal legislation related to consumer protection issues. This is helpful for states to use as a guide to create their own legislation if necessary.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. JERRY MORAN TO HON. MIKE DEWINE

Question. There are a number of state attorneys general that have made public service announcements (PSAs) warning consumers of the dangers to their finances and cybersecurity from visiting pirate websites, and many are in the process of amending their websites to reflect this. Do you think the state Attorneys General, as well as the FTC, has a role in these efforts?

Answer. My office does a tremendous amount of outreach and education relating to cybersecurity and online scams of all types. In spite of our efforts, Ohioans continue to be victimized by pirated websites, phony friend requests, and bogus online offers.

There are nearly endless opportunities to reach consumers in their homes, on their mobile devices, and through traditional and social media. Having a diversity of sources and voices can be very beneficial to our efforts to help consumers protect themselves from frauds and scams.

Messages from Attorneys General can be reinforced by messages from the Federal Trade Commission, and vice versa. There is plenty of room in this arena for state Attorneys General and for the Federal Trade Commission. Each brings value and consumers deserve that maximum opportunity to learn about risks they may face while online. The FTC has always promoted states using the FTC resources—such as publications and videos—at no cost to the state. With the FTC’s abilities to make high-end videos, it’s helpful to the states who have limited resources to produce videos; the same can be said about their publications.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TODD YOUNG TO HON. MIKE DEWINE

Question 1. Mr. DeWine, what have you experienced in neighboring Ohio relative to travel booking scams and what additional support do you believe you could use from the FTC?

Answer. We have experienced some travel booking scams or complaints, but we do not see a large majority of complaints from this specific category. That’s not to say we don’t take action. In 2013, we had a number of complaints against an individual who accepted money for vacations booked through her, but she provided nothing. In that case, we worked with the local prosecutor to prosecute her for two counts of theft, one of which she eventually plead guilty.

While Ohio has the ability to bring cases on its own, as well as with other states, the FTC could be instrumental in helping curb bad practices of larger nation-wide businesses. For example, the FTC could help set best practices for third-party booking sites, vacation club memberships, or additional fees imposed by travel booking sites.

Question 2. Mr. DeWine, has the FTC focused in on the issue of travel booking scams beyond issuing consumer alerts?
Answer. Currently, I’m unaware of any cases the FTC is involved with regarding travel booking scams; that is not to say, however, that there are not cases. I do know that in January 2017, the FTC took a strong stance against and suggested legislation regulating additional fees imposed by hotels and resorts in which the hotel or resort was advertising a lower rate but then adding on an additional fee as “resort fee.”

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. BILL NELSON TO HON. MIKE DÉWINE

Question. On this Committee, we often consider consumer-protection bills in which state attorneys general play a role in enforcement. For me, I believe multiple “cops on the beat” are a good thing, and I always support legislation where state attorneys general can partner with Federal agencies to work on the American people’s behalf. However, some bills we consider in this Committee attempt to preempt state consumer-protection laws and clip the wings of state attorneys general’s authorities. Can you comment on how important it is to preserve the prerogatives of state attorneys general to protect consumers from scams and fraud?

Answer. It is imperative that the states’ authority to protect consumers is preserved. The attorneys general are uniquely situated to address scams and unfair or deceptive practices at the regional, state, and local levels. Many times bad actors target specific geographic areas or populations within a state to take advantage of a disaster, weather event, or unique market. The attorneys general can react to these problems much more quickly and decisively than a Federal agency.

In many ways, the attorneys general are the first line of defense for all Americans, as the enforcement actions taken on the state level influence practices across the spectrum of businesses inside our states and out.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. RICHARD BLUMENTHAL TO HON. MIKE DÉWINE

Question. The FTC’s “Every Community Initiative” recognizes that fraud affects every community, and creates consumer education materials for vulnerable and often targeted communities, including older adults, military families, immigrants, and members of the Latino community. Would it be fair to say that if our efforts to educate consumers and small businesses about scams were reduced or discontinued, the American economy would suffer even more financial loss as a result of scams?

Answer. I can’t speak to the value of any single program, but I can talk about consumer education as a whole. I believe in the value of having staff assigned to helping people understand how they can avoid falling victim to a scam or making a bad purchasing decision and assisting them with recovering after it’s happened. In Ohio, we put a lot of effort into finding ways to communicate with our consumer and business communities, including our immigrant and non-English speaking communities. We do this through social media, targeted outreach, and by having staff out in the field meeting people where they live. We are, first and foremost, public servants and we must do what it takes to protect the families and businesses we serve.

Although we appreciate the efforts the FTC has made, the attorneys general understand that it’s our job to educate our consumers. We will continue to fulfill our obligations no matter what happens to any specific Federal program.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. BILL NELSON TO FRANK W. ABAGNALE, JR.

Question 1. In your various writings over the years, you make a passionate case about the growth and harms of identity theft and the need for Federal legislation to tackle the problem. For instance, in The Art of the Steal, you wrote, “If we’re serious about combating identity theft, it’s going to take a Federal solution [. . .].” In Stealing Your Life—in a chapter titled, “Write Your Company and Congressperson—Now!”—you wrote, “Congress and state legislatures need to provide consumers with more protection.” Do you continue to believe that there must be a Federal solution?

Answer. Yes, I do. I believe there needs to be Federal laws on the books that hold companies, corporations and financial institutions liable for breaches that occur due to their negligence. The same way I feel very strongly that companies that produce software and hardware be responsible when their technology does not protect indi-
viduals, as well as businesses, when they claim it was designed to do so. Having no legal recourse, individuals, as well as businesses, are left in harm’s way when companies do not take the adequate and necessary steps to make sure that there are no loop holes in their technology. For example, over the past 20 years I have worked as an advisor on two great fraud prevention technologies. The first one was called the 41st Parameter, eventually sold to Experian and now used in 80 countries around the world by governments, banks, corporations, airlines, and retailers. I am currently finishing a technology called Trusona (www.trusona.com) which does away with passwords and has become the only insured verification technology in the world insured by an A+ insurance company. We were able to obtain this insurance because we allowed the insurance company to spend over a year testing the technology in various labs around the world to see if it could be defeated before allowing it to be insured. Even in the paper/print side, more than 10 years ago I designed a high security check for a California security printer known today as the Supercheck (www.safechecks.com). Today, that check is used by thousands of corporations, state and city governments and has never been counterfeited, altered or forged.

I work with technology companies because they can’t think like a criminal. Through I can’t write code, I can play “chess” with them until I’ve taken away every possibility of defeating the technology. I know this can be done, having done it, so I believe all companies should be responsible for taking the necessary steps to ensure their technology works instead of rushing to market just to make a buck at the consumer’s risk.

**Question 2.** As you may or may not know, I introduced legislation with Senator Blumenthal last Congress—S. 177, the Data Security and Breach Notification Act of 2015—that would require companies holding large amounts of personal information to take reasonable security measures and would establish a uniform Federal standard for breach notification. In concept, what are your thoughts, if any, on this type of Federal solution?

**Answer.** I would be absolutely 100 percent behind this bill. Again, there is no reason that companies cannot take the time and expense to educate their employees about the most important job they have. That is protecting the private and sensitive information they have that has been entrusted to them by their customers and clients. This means training everyone from the custodian to the CEO. Over the last 40 years, I’ve had the opportunity to make presentations to many Fortune 500 Companies who understand that education is the most powerful tool to fight fraud and cybercrimes. If I company or institution is not willing to put the interest and protection of their clients and customers first, then they should be held responsible. I support this bill.

As a way of example, the Federal Government could do a much better job of protecting the taxpayers’ money and information. I always believe that the government should take the lead and the rest of the country will follow.

**RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. RICHARD BLUMENTHAL TO FRANK W. ABAGNALE, JR.**

**Question.** The FTC’s “Every Community Initiative” recognizes that fraud affects every community, and creates consumer education materials for vulnerable and often targeted communities, including older adults, military families, immigrants, and members of the Latino community.

Would it be fair to say that if our efforts to educate consumers and small businesses about scams were reduced or discontinued, the American economy would suffer even more financial loss as a result of scams?

**Answer.** Yes, it would and already has. As I mentioned in my testimony, in the last 1970s I was featured in a number of public service ads sponsored by the DOJ that were sent out to law enforcement agencies on tips for protecting consumers on subjects like protecting their check book, their credit cards, and personal assets. I donated my time to this project as I knew how important it was. Those PSAs ran for a number of years and were very effective.

In the mid-1980s I allowed by intellectual property to be used by a large bank financial printer for bank statement stuffers with tips for consumers. Hundreds of banks sent these statement stuffers to hundreds of thousands of individuals as just a public service message from their bank. In both of those projects, I was not known by very many people but they were still very effective.

I strongly believe that the government, through agencies like the FTC, should begin a public awareness program about consumer crimes and safety in the cyber world. As in the past, I will always be willing to provide my services and intellectual
property to a government initiative like this at absolutely no cost or travel expenses
to accomplish this. Whether the government choses me as their spokesman or not,
I absolutely stand behind the initiative to create consumer educational materials
targeted to communities, older adults, military families, immigrants and members
of the Latino community.

I’d like to make one final point. In the last couple of years, I have actually do-
nated my time and travel to film some public service ads for the DOJ National Ad-
 vocacy Center (NAC), as well as the Association of State Attorneys General. Unfor-
 tunately, there was no money put behind these ads, they were poorly filmed and
produced and consequently, ended up being shown only on government websites. If
the government decides to create a campaign for public awareness, they must put
the money behind it so it is professionally done so that network and cable TV will
show it.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. RICHARD BLUMENTHAL TO
MIKE SCHWANKE

Question. The FTC’s “Every Community Initiative” recognizes that fraud affects
every community, and creates consumer education materials for vulnerable and
often targeted communities, including older adults, military families, immigrants,
and members of the Latino community.

Would it be fair to say that if our efforts to educate consumers and small busi-
 nesses about scams were reduced or discontinued, the American economy would suf-
fer even more financial loss as a result of scams?

Answer. My name is Michael Schwanke with KWCH TV in Wichita, Kansas. In
my 17 years as a journalist and investigative reporter I have focused much of time
on helping victims of scams and educating the public so they don’t fall victim.

To answer your question, I believe that education is the best weapon we have to
prevent scams. Enforcement is often impossible as the scammers change tactics
daily and operate from other countries.

As I stated in my testimony, the education has to be consistent. We have seen
viewers fall for scams even after they’d been warned.

I personally have seen seniors wire away their entire life savings to scammers.
Everyone, including the Federal Government, has a role in preventing the next per-
son from falling victim.

I appreciate the opportunity to share my experience.