

**CYBER CRIMINALS AND FRAUDSTERS:
HOW BAD ACTORS ARE EXPLOITING
THE FINANCIAL SYSTEM DURING
THE COVID-19 PANDEMIC**

VIRTUAL HEARING
BEFORE THE
SUBCOMMITTEE ON NATIONAL SECURITY,
INTERNATIONAL DEVELOPMENT AND
MONETARY POLICY
OF THE
COMMITTEE ON FINANCIAL SERVICES
U.S. HOUSE OF REPRESENTATIVES
ONE HUNDRED SIXTEENTH CONGRESS
SECOND SESSION

JUNE 16, 2020

Printed for the use of the Committee on Financial Services

Serial No. 116-96



U.S. GOVERNMENT PUBLISHING OFFICE

42-896 PDF

WASHINGTON : 2021

HOUSE COMMITTEE ON FINANCIAL SERVICES

MAXINE WATERS, California, *Chairwoman*

CAROLYN B. MALONEY, New York	PATRICK McHENRY, North Carolina,
NYDIA M. VELAZQUEZ, New York	<i>Ranking Member</i>
BRAD SHERMAN, California	ANN WAGNER, Missouri
GREGORY W. MEEKS, New York	FRANK D. LUCAS, Oklahoma
WM. LACY CLAY, Missouri	BILL POSEY, Florida
DAVID SCOTT, Georgia	BLAINE LUETKEMEYER, Missouri
AL GREEN, Texas	BILL HUIZENGA, Michigan
EMANUEL CLEAVER, Missouri	STEVE STIVERS, Ohio
ED PERLMUTTER, Colorado	ANDY BARR, Kentucky
JIM A. HIMES, Connecticut	SCOTT TIPTON, Colorado
BILL FOSTER, Illinois	ROGER WILLIAMS, Texas
JOYCE BEATTY, Ohio	FRENCH HILL, Arkansas
DENNY HECK, Washington	TOM EMMER, Minnesota
JUAN VARGAS, California	LEE M. ZELDIN, New York
JOSH GOTTHEIMER, New Jersey	BARRY LOUDERMILK, Georgia
VICENTE GONZALEZ, Texas	ALEXANDER X. MOONEY, West Virginia
AL LAWSON, Florida	WARREN DAVIDSON, Ohio
MICHAEL SAN NICOLAS, Guam	TED BUDD, North Carolina
RASHIDA TLAIB, Michigan	DAVID KUSTOFF, Tennessee
KATIE PORTER, California	TREY HOLLINGSWORTH, Indiana
CINDY AXNE, Iowa	ANTHONY GONZALEZ, Ohio
SEAN CASTEN, Illinois	JOHN ROSE, Tennessee
AYANNA PRESSLEY, Massachusetts	BRYAN STEIL, Wisconsin
BEN McADAMS, Utah	LANCE GOODEN, Texas
ALEXANDRIA OCASIO-CORTEZ, New York	DENVER RIGGLEMAN, Virginia
JENNIFER WEXTON, Virginia	WILLIAM TIMMONS, South Carolina
STEPHEN F. LYNCH, Massachusetts	VAN TAYLOR, Texas
TULSI GABBARD, Hawaii	
ALMA ADAMS, North Carolina	
MADELEINE DEAN, Pennsylvania	
JESUS "CHUY" GARCIA, Illinois	
SYLVIA GARCIA, Texas	
DEAN PHILLIPS, Minnesota	

CHARLA OUERTATANI, *Staff Director*

SUBCOMMITTEE ON NATIONAL SECURITY, INTERNATIONAL
DEVELOPMENT AND MONETARY POLICY

EMANUEL CLEAVER, Missouri, *Chairman*

ED PERLMUTTER, Colorado
JIM A. HIMES, Connecticut
DENNY HECK, Washington
BRAD SHERMAN, California
JUAN VARGAS, California
JOSH GOTTHEIMER, New Jersey
MICHAEL SAN NICOLAS, Guam
BEN McADAMS, Utah
JENNIFER WEXTON, Virginia
STEPHEN F. LYNCH, Massachusetts
TULSI GABBARD, Hawaii
JESÚS "CHUY" GARCIA, Illinois

FRENCH HILL, Arkansas, *Ranking Member*
FRANK D. LUCAS, Oklahoma
ROGER WILLIAMS, Texas
TOM EMMER, Minnesota
ANTHONY GONZALEZ, Ohio
JOHN ROSE, Tennessee
DENVER RIGGLEMAN, Virginia, *Vice
Ranking Member*
WILLIAM TIMMONS, South Carolina
VAN TAYLOR, Texas

CONTENTS

	Page
Hearing held on:	
June 16, 2020	1
Appendix:	
June 16, 2020	35

WITNESSES

TUESDAY, JUNE 16, 2020

Coleman, Kelvin, Executive Director, National Cyber Security Alliance	9
Jaffer, Jamil N., Founder and Executive Director, National Security Institute, and Assistant Professor of Law and Director, National Security Law & Policy Program, Antonin Scalia Law School, George Mason University	10
Kellermann, Tom, Head, Cybersecurity Strategy, VMware, Inc.	5
Senn, Amanda, Chief Deputy Director, Alabama Securities Commission, and Chair, Cybersecurity Committee, North American Securities Administrators Association (NASAA), on behalf of NASAA	7

APPENDIX

Prepared statements:	
Coleman, Kelvin	36
Jaffer, Jamil N.	41
Kellermann, Tom	53
Senn, Amanda	57

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

Cleaver, Hon. Emanuel:	
Written statement of Americans for Financial Reform	68
Written statement of NAFCU	69
Written statement of Third Way	71
Gottheimer, Hon. Josh:	
Letters of support from various organizations for the Senior Investor Pandemic and Fraud Protection Act	116
Hill, Hon. French:	
Written statement of the American Securities Association	134
Written statement of the Consumer First Coalition	140
Jaffer, Jamil:	
Written responses to questions for the record from Representative Hill	142
Kellermann, Tom:	
Written responses to questions for the record from Representatives Perl- mutter and Hill	145

**CYBER CRIMINALS AND FRAUDSTERS:
HOW BAD ACTORS ARE EXPLOITING
THE FINANCIAL SYSTEM DURING
THE COVID-19 PANDEMIC**

Tuesday, June 16, 2020

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON NATIONAL SECURITY,
INTERNATIONAL DEVELOPMENT
AND MONETARY POLICY,
COMMITTEE ON FINANCIAL SERVICES,
Washington, D.C.

The subcommittee met, pursuant to notice, at 12:01 p.m., via Webex, Hon. Emanuel Cleaver [chairman of the subcommittee] presiding.

Members present: Representatives Cleaver, Perlmutter, Himes, Heck, Sherman, Vargas, Gottheimer, Wexton, Lynch, Garcia of Illinois; Hill, Lucas, Williams, Emmer, Gonzalez of Ohio, Rose, Timmons, and Taylor.

Ex officio present: Representative Waters.

Chairman CLEAVER. The Subcommittee on National Security, International Development and Monetary Policy will come to order.

Without objection, the Chair is authorized to declare a recess of the subcommittee at any time.

Also, without objection, members of the full Financial Services Committee who are not members of this subcommittee are authorized to participate in today's hearing.

Members are reminded to keep their video function on at all times, even when they are not being recognized by the Chair. Members are also reminded that they are responsible for muting and unmuting themselves, and to mute themselves after they have finished speaking.

Consistent with the regulations accompanying H. Res. 965, staff will only mute Members and witnesses as appropriate when not recognized to avoid inadvertent background noise. Members are reminded that all House rules relating to order and decorum apply to this remote hearing.

Today's hearing is entitled, "Cyber Criminals and Fraudsters: How Bad Actors Are Exploiting the Financial System During the COVID-19 Pandemic."

I now recognize myself for 4 minutes for an opening statement.

Let me, first of all, thank Lisa and the rest of the committee staff who have worked so hard to make this and all of our committee hearings possible.

As the pandemic continues to move through our communities and our country, and to devastate the physical health of our citizens, it has managed to also infect the economic health of our nation.

Congress, through a bipartisan effort, passed the CARES Act, which unlocked unprecedented relief to families and small businesses, relief that, according to the Federal Reserve, may not be enough to prevent a long and protracted economic downturn. Nevertheless, significant investments were made to rescue millions of working citizens.

In this time of suffering and hardship for so many, we are seeing criminal actors here at home and around the world redoubling their efforts to target families, financial institutions, and even arteries of government.

Poverty and exploitation are indivisible evils. They have been long-time sidekicks. Just last month, the FBI unsealed a criminal indictment of what looks to be the first case of COVID-19-related money laundering and fraud brought by the Department of Justice. The criminal charge relates to a healthcare provider claiming to offer free COVID tests, but billions of Medicare dollars are being wasted.

According to the Federal Trade Commission, there are nearly 1,000 reports of COVID-19-related fraud totaling over \$0.5 million in my home State of Missouri. This is a fraction of the nearly 100,000 fraud reports nationwide totaling \$60 million reported by the Commission. I would like to highlight that these reports do not even fully capture the full landscape of COVID-19-related fraud.

The FBI's Criminal Investigative Division notes that there has been potentially \$126 million in Paycheck Protection Program (PPP) fraud. We are seeing a 75-percent spike in daily cybercrimes reported by the FBI since the start of the pandemic. The Financial Crimes Enforcement Network (FinCEN) is doing what it can by putting out advisories warning consumers and financial institutions of the proliferation of criminal schemes.

Last month, FinCEN released warnings of COVID-related medical schemes in what would be the first of several advisories that FinCEN intends to issue concerning financial crimes relating to the COVID-19 pandemic. However, it is abundantly clear that our financial security systems are being taxed right now.

The FBI, in their testimony before the Senate Judiciary Committee last week, noted that the sheer volume of complaints that the Internet Crime Complaint Center is receiving is presenting a challenge for the FBI's criminal program. In response, the FBI started a PPP Fraud Working Group with the Department of Justice and the Small Business Administration's Inspector General to triage the overwhelming caseload.

The thieves and fraudsters that are targeting consumers are not just at home, but they are indeed everywhere. International law enforcement coordinating agencies, Interpol and Europol, have highlighted their efforts to target cross-border criminals.

There is some positive news. We have done something to help address this as a committee and as a Chamber. Last year, we unanimously passed through the House the COUNTER Act. The bill closed a number of loopholes that have allowed financial crimes to

be committed, and pulls us into the 21st Century by positioning the U.S. to face tomorrow's challenges.

I look forward to hearing from all of you on these important issues.

The Chair now recognizes the ranking member of the subcommittee, the gentleman from Arkansas, Mr. Hill, for 4 minutes for an opening statement.

Mr. HILL. I thank the chairman. I appreciate you convening this virtual hearing. And I appreciate the witnesses being with us today to share their expertise.

Mr. Chairman, I have a letter from the American Securities Association that I would like to enter into the record. Thank you very much.

Chairman CLEAVER. Without objection, it is so ordered.

Mr. HILL. Thank you. I appreciate our ability to innovate. My thanks, too, to the staff for providing this foundation for our virtual hearings.

We had a roundtable a few days ago on this topic, and I thank the chairman for holding this formal hearing and returning to this topic. It is an important dialogue as it relates to our constituents: national security. And featuring it in a hearing means that our discussion will be cataloged in our official records.

As we continue our essential work, I do hope that in the coming months, we are able to hold bipartisan hearings on the following topics that I think are important before our committee.

First of all, the Committee on Foreign Investment in the United States (CFIUS). We are required annually to conduct oversight on CFIUS, and we made significant reforms in the last Congress, and I hope we can have a hearing on that.

Also, monetary policy. We will be having Federal Reserve Chair Jay Powell before the Full Committee this week, but I think it is important for us to look at monetary policy in the face of the unprecedented actions taken by the Fed to expand its balance sheet.

And finally, the international financial institutions and how they are responding to COVID-19 across the world, particularly in our emerging markets.

I thank the chairman for the opportunity to work on these issues for future hearings.

Cybersecurity and the need for strong cyber protocols has long been a topic of discussion in this committee, and the virus has only underscored the need and showcased the vulnerabilities that we have in certain aspects of our financial ecosystem.

According to the FBI Internet Crime Complaint Center (IC3), the number of cybersecurity complaints to the IC3 in the last 4 months has spiked from typically 1,000 daily before the pandemic to as many as 4,000 incidents a day.

Furthermore, a survey conducted last month by VMware Carbon Black, one of our witnesses today, found that 80 percent of surveyed banks reported year-on-year increases in cyber attacks within the financial services sector. This year, those attacks have surged 238 percent from February to April.

As many businesses and financial institutions are adapting to the new teleworking policies and the challenges that come from working remotely, it is imperative that they have the right infra-

structure in place to handle new security protocols and sensitivities.

Just last week, the FBI announced that bad actors are seeking to exploit customers through mobile banking, and recommended that consumers take proper precautions.

These attacks can take various shapes and infiltrate in a variety of ways, even here in Arkansas. I noted in the roundtable a few weeks ago that we had a PPP program that was a fraud attempt. Fortunately, that person has been arrested and charged with bank fraud.

I look forward to hearing from our witnesses today on how we can best combat these accounts.

Before I close, I would like to quickly touch on China and the threat to cybersecurity. The U.S. has been the target of cyber attacks from nation-states and nonstate actors for over 20 years. But in the months of outbreak in the virus in the United States, cyber espionage from China, Russia, and Iran has spiked. Cyber threat actors are taking advantage of this crisis to attempt to undermine the U.S. Government and probe our systems in the private sector and public sector for weakness, and to stoke fear and division and confusion here at home.

According to the FBI, China has been observed attempting to identify and illicitly obtain valuable intellectual property (IP), and public health data related to vaccine treatments and testing from our networks throughout our country. We cannot allow the actions of a few bad actors and foreign threats to inhibit our financial institutions.

I thank the Chair. I yield back, and I look forward to the discussion today.

Chairman CLEAVER. Today, we welcome the testimony of, first, Mr. Tom Kellermann. Mr. Kellermann currently serves as the chief cybersecurity officer for VMware Carbon Black. Prior to this, he was the CEO and founder of Strategic Cyber Ventures, and served as the Commissioner on President Barack Obama's Commission on Cybersecurity.

In 2003, he coauthored the book, "Electronic Safety and Soundness: Securing Finance in a New Age." And in 2017, he was appointed as the Wilson Center's Global Fellow for Cyber Policy. Thank you for appearing before this subcommittee.

Second, we have Mr. Kelvin Coleman. Mr. Coleman currently serves as executive director of the National Cyber Security Alliance, an organization focused on cybersecurity awareness for home users, businesses, and educational institutions. Mr. Coleman comes to this position with 20 years of experience. He served in the White House, having worked on President Bush's and President Obama's National Security Telecommunications Advisory Committee and National Security Staff, the U.S. Department of Homeland Security, as well as the private sector. Thank you for appearing before this subcommittee.

Third, we have Ms. Amanda Senn. Ms. Senn is testifying on behalf of the North American Securities Administrators Association (NASAA), where she chairs their Cybersecurity Committee. NASAA represents State and provincial security regulators in the United States, Canada, and Mexico. NASAA members are the clos-

est regulators to local communities, small businesses, and the investing public throughout North America. Ms. Senn is also the chief deputy director of the Alabama Securities Commission, the State securities regulator. Thank you for appearing before this subcommittee.

And fourth, Mr. Jamil Jaffer currently serves as the founder and executive director of the National Security Institute. He is also assistant professor of law and the director of the National Security Law and Policy Program at the Antonin Scalia Law School at George Mason University. Additionally, he is vice president of IronNet Cybersecurity, a startup technology firm. Prior to these positions, he served as Senior Counsel on the House Permanent Select Committee on Intelligence under Chairman Mike Rogers, as well as Assistant Counsel to the President in the Bush Administration. Thank you for appearing before the subcommittee.

Witnesses are reminded that your oral testimony will be limited to 5 minutes. A chime will go off at the end of your time, and I ask that you respect the members' and the other witnesses' time by wrapping up your oral testimony.

And without objection, your written statements will be made a part of the record.

Mr. Kellermann, you are now recognized for 5 minutes to give an oral presentation of your testimony.

STATEMENT OF TOM KELLERMANN, HEAD, CYBERSECURITY STRATEGY, VMWARE, INC.

Mr. KELLERMANN. Thank you.

Chairman Cleaver, Ranking Member Hill, members of the subcommittee, I am Tom Kellermann, head of cybersecurity strategy for VMware, Inc. Thank you for the opportunity to testify again before the subcommittee today.

America is grappling with a cyber insurgency, and our financial sector is the number one target. A recent report issued by the World Economic Forum states that the dark web economy of scale will be the third-largest economy in the world by 2021.

During the first 5 months of 2020 alone, cyber attacks against the financial sector have increased by 238 percent. This is compounded by the 900-percent increase in ransomware attacks. Cyber criminals are capitalizing on COVID-19, and they are doing so in tandem with the news cycle.

Over the past 6 months, cyber defenders have seen a high level of coordination from cyber criminals who are demonstrating significant innovation to maintain persistent and even counter-incident response efforts. This includes ransomware campaigns, business email compromise scams, and access mining.

Criminals are increasingly sharing resources and information and reinvesting their illicit profits into the development of new and even more destructive capabilities. The cybercrime community has educated themselves as to the interdependencies that exist in the financial sector, and they have begun to commandeer these very interdependencies to manifest criminal conspiracies.

Thirty-three percent of surveyed financial institutions said that they have encountered, "island hopping." This is an attack where the supply chains and partners are commandeered to target the

primary financial institution. Once that bank is compromised, the criminals use the digital infrastructure to attack that bank's customers. It is also notable that a few rogue nation-states are offsetting economic sanctions via attacks on our payment systems.

The international financial system is constantly facing new threats as technology proliferates and diversifies. There is an increasing number of security breaches and thefts on digital currency exchange platforms, as well as the misuse of these platforms by cybercriminals to launder stolen money. Dark web forums enabled by anonymous virtual currencies have created a bazaar for criminals and organized crime to reach a global market.

In addition to organized crime, extremist organizations are also known to use alternative payment systems for operational purposes and to raise funds. Many of these payment systems and cryptocurrencies offer true or relative anonymity. This raises the necessity of increased regulation of digital money.

In 2020, cybercrime conspiracies will become increasingly punitive and destructive. In fact, one out of four cyber attacks today are destructive.

Fintech firms themselves present significant operational risks, lacking the proper incentive for proper intrusion detection as well as "know thy customer" anti-money-laundering protocols under the Bank Secrecy Act.

Given that 50 percent of all crimes now have a cyber component, it is high time that we follow the money to create an international e-forfeiture fund.

The modern epidemic of cybercrime and cyber espionage can be mitigated through modernization of existing authorities to combat cyber money laundering. Virtual currencies and other alternative payment systems that facilitate money laundering associated with existing cybercrimes, as well as terrorist financing, must be held to account.

In closing, the safety and soundness of the financial sector is dependent on proactive policy. I would like to highlight six opportunities for legislative actions for the subcommittee's consideration.

First, any money laundering and forfeiture regulations must be modernized to seize the virtual currencies and digital payments which are used in cybercrime conspiracies.

Second, I ask the House to pressure the Senate to pass the COUNTER Act, H.R. 2514, that passed out of the House under Chairman Cleaver's leadership.

Third, charge the Financial Stability Oversight Council (FSOC) with the responsibility to create a framework for regulating cryptocurrencies and developing guidelines for strong protections against money laundering and cyber threats to those marketplaces.

Fourth, elevate chief information security officers to directly report to the CEOs of financial institutions.

Fifth, establish a tax credit for financial sector companies to dedicate at least 10 percent of their IT budgets towards cybersecurity.

And lastly, support the House passage of S.3636, the United States Secret Service Mission Improvement and Realignment Act of 2020, which moves the Secret Service back to its original home at the Department of the Treasury.

Chairman Cleaver, Ranking Member Hill, thank you for the opportunity to participate in this morning's important hearing. I am happy to answer any questions the subcommittee may have.

[The prepared statement of Mr. Kellermann can be found on page 53 of the appendix.]

Chairman CLEAVER. Thank you, Mr. Kellermann.

Ms. Senn, you are now recognized for 5 minutes to give an oral presentation of your testimony.

STATEMENT OF AMANDA SENN, CHIEF DEPUTY DIRECTOR, ALABAMA SECURITIES COMMISSION, AND CHAIR, CYBERSECURITY COMMITTEE, NORTH AMERICAN SECURITIES ADMINISTRATORS ASSOCIATION (NASAA), ON BEHALF OF NASAA

Ms. SENN. Good morning, Chairman Cleaver, Ranking Member Hill, and members of the subcommittee. My name is Amanda Senn, and I am chief deputy director of the Alabama Securities Commission, and Chair of the Cybersecurity Committee for the North American Securities Administrators Association, or NASAA. I am pleased to testify today before the subcommittee on behalf of NASAA.

States are leaders in prosecuting securities violations, and our focus is on protecting retail investors. History has shown that opportunistic fraudsters will use COVID-19, much as they have in other crises, to fleece mom-and-pop investors.

Acting within the framework of NASAA, State securities regulators have formed a task force to root out and shut down fraud related to COVID-19. This initiative is being led by NASAA's Enforcement Committee and includes more than 100 investigators from the vast majority of our member jurisdictions.

The objective of this task force is to disrupt, discourage, and deter fraudulent or illegal activities which pose threats to investors before significant losses can occur. This task force is proactively protecting investors against fraud through the broad dissemination of enforcement orders, notices, and warnings.

As the subcommittee is aware, the proliferation of technology has changed how we solicit, manage, and communicate with those handling our investments. For that reason, this task force is using online investigative techniques to identify websites and social media posts that may be offering or promoting investment fraud or unregistered regulated activities.

Unfortunately, though, fraudsters are evolving with technology. For example, earlier this month, my office received three separate reports pursuant to Alabama's financial exploitation reporting law, which indicated individuals had become victims of an online fraud scheme.

These victims had visited the web page of a very reputable broker, and they discovered they were unable to log in. Upon their attempts, they received a screen with a help button. The individuals were instructed to call a 1-800 number, and the person who answered the phone told the victims that the broker's website was down because 5G towers were being placed in California.

That person then instructed the callers to log into their accounts with information that was provided by the suspect. The victims

logged in as instructed, and shortly thereafter, wire transfers were initiated from their account to overseas banking accounts.

During an interview with the firm last Friday, our case agent learned that \$1.2 million had already been stolen from the accounts of investors. It is believed that malware was responsible for redirecting the victims from the legitimate web page to the fraudulent knockoff site.

To date, at least 84 victims nationwide have been impacted, and the numbers continue to rise. At one time, this crime would have likely been perpetrated by a person that local authorities could readily identify through the use of subpoenas and search warrants. In the digital age, however, regulators are confronted with numerous evidentiary challenges which, given limited resources, make it difficult to investigate and prosecute these cases.

States are, however, committed to our investor protection mission regardless of the means used to rip off our investors.

The committee has invited NASAA to share its views regarding legislative proposals that have been posted in connection with today's hearing. I want to just mention two.

The first is the Senior Investor Pandemic and Fraud Protection Act. This would implement the Senior Investor Protection Grant Program that was originally authorized by Section 989(A) of the Dodd-Frank Act, but was never put into effect.

This bill would also expand the scope of the grant to include frauds related to COVID-19. And under the bill, State regulators could apply for up to \$500,000 annually in grant funding to combat financial fraud of seniors and vulnerable adults in cases related to the pandemic. This would extend for a maximum of 2 years.

The grant funds could be used to hire staff to investigate fraudulent conduct, to acquire technology and equipment, and to train investigators and prosecutors to target COVID-19 fraud, and also to provide important educational materials to seniors and vulnerable adults.

NASAA strongly supports this bill, and so do at least 11 other organizations, and we urge Congress to act on it.

The second is the COVID-19 Restitution Assistance Fund for Victims of Securities Violations Act, which would create a fund at the SEC to provide restitution payments for individuals in connection with securities fraud related to coronavirus if they do not otherwise receive full restitution. As you can imagine, in financial fraud cases, once the money is gone, often, it is never recovered.

Some States have enacted similar legislation with great success, and we strongly support this bill.

Thank you again for the opportunity to testify, and I will be pleased to answer any questions you may have.

[The prepared statement of Ms. Senn may be found on page 57 of the appendix.]

Chairman CLEAVER. Thank you for your testimony, Ms. Senn.

Mr. Coleman, you are now recognized for 5 minutes to give an oral presentation of your testimony.

**STATEMENT OF KELVIN COLEMAN, EXECUTIVE DIRECTOR,
NATIONAL CYBER SECURITY ALLIANCE**

Mr. COLEMAN. Chairman Cleaver, Ranking Member Hill, and members of the subcommittee, thank you for inviting me to today's hearing. It is a pleasure to join Tom, Amanda, and Jamil.

My name is Kelvin Coleman, and I am the executive director of the National Cyber Security Alliance (NCSA). NCSA's core mission is to build strong public-private partnerships to create and implement broad-reaching cybersecurity, education, and awareness initiatives.

The United States confronts a dangerous combination of both known and unknown cyber vulnerabilities. We face adversaries who are strong and rapidly expanding with ever-increasing cyber capabilities to breach our networks.

During today's hearing, we will examine cyber threats and the bad actors who are exploiting the COVID-19 crisis. We will have robust discussions of tools, techniques, and procedures used by these bad actors. And we will certainly deliberate on the products and processes we put into place to mitigate those challenges.

And while products and processes are important, I believe we need to focus even more on encouraging and supporting partnerships. I am going to talk a lot about partnerships today, and that is exactly what the National Cyber Security Alliance focuses on.

In the words of Michael Madden of Mimecast, NCSA is the lead in building community defense through partnerships for our nation.

This is especially true during the COVID-19 era. Tonia Dudley and her team at Cofense are seeing threat actors that continue to exploit the Paycheck Protection Program and SMB funding initiatives in several sophisticated phishing campaigns.

Because of this type of threat and many others, NCSA, our board companies, Federal partners, and nonprofit collaborators have worked swiftly to provide organizations and individuals with relevant and helpful information to help address security and privacy concerns during the global COVID-19 outbreak. We have built what we call the COVID Security Resource Library, and folks have found it extraordinarily helpful.

And with the help of companies like Trend Micro and Generali Global Assistance, we also created a COVID-19 webinar series for small and medium-sized businesses.

Of course, bad actors were committing malicious acts before COVID-19, and they will certainly do so after this crisis subsides.

To deal with threats in our continuously connected society, NCSA leads a number of other initiatives, including Cybersecurity Awareness Month, Data Privacy Day, and the CyberSecurity My Business program.

And while these programs and resources provide tremendous value in the fight to protect Americans, I will say it again: partnerships are our biggest assets. And the private sector is incredibly important in this fight.

The Federal Government plays an equally important role in cybersecurity and educational awareness. Chief among NCSA's Federal partners is the Cybersecurity and Infrastructure Security Agency (CISA). They have been very helpful in the fight to help

Americans secure their networks. And I must say, CISA is very engaged, very responsive, and very supportive overall.

NCSA, in coordination with our partners, has put a lot of effort into building a more secure, interconnected world. In the words of Kristina Dorville at AIG, bad actors are communicating, and bad actors are coordinating, so why shouldn't the good guys?

With that said, there is still so much to be done. Congress should consider making game-changing investments into cybersecurity awareness and education, investments that could benefit the American people as well as the small and medium-sized business community.

As Americans begin to rely more heavily on telework, bad actors will increase their malicious activities and target those working from home. Americans must be equipped with the knowledge to protect themselves, their families, and their communities. Congress can and should play an important role in making sure Americans understand the many dangers of inadequately securing their systems, devices, and information.

Thank you, Mr. Chairman, and I look forward to answering the subcommittee's questions.

[The prepared statement of Mr. Coleman can be found on page 36 of the appendix.]

Chairman CLEAVER. Thank you, Mr. Coleman.

Mr. Jaffer, you are now recognized for 5 minutes to give an oral presentation of your testimony.

STATEMENT OF JAMIL N. JAFFER, FOUNDER AND EXECUTIVE DIRECTOR, NATIONAL SECURITY INSTITUTE, AND ASSISTANT PROFESSOR OF LAW AND DIRECTOR, NATIONAL SECURITY LAW & POLICY PROGRAM, ANTONIN SCALIA LAW SCHOOL, GEORGE MASON UNIVERSITY

Mr. JAFFER. Thank you, Mr. Chairman. Thank you, Chairman Cleaver, Ranking Member Hill, and members of the subcommittee, for being here today and for inviting me to talk about the very real threats that face our nation and the U.S. financial sector and those of our allied nations.

As you know, the threats to our financial sector have been real and serious for decades. They have become particularly problematic in the context of the current pandemic.

I want to note your leadership, Mr. Chairman, for calling out the very real threat of Iranian attacks on the United States, including on our financial infrastructure, for protecting our oil and natural gas pipeline infrastructure, and for fighting actively against overt and covert disinformation efforts online, including those that seek to divide us as a nation.

In addition, Ranking Member Hill, I want to thank you for your leading efforts on identity theft, for your sanctions against Russia for its meddling in the 2016 election, and for your efforts to press NATO to extend its security umbrella to cover cyberspace, and ensuring that we continue to enjoy and innovate the military superiority in the cyber arena.

I think it is critical today that we identify the very real threats that we face as a nation in the financial sector and take action immediately to address them. In a 2019 letter to shareholders, the

CEO of JPMorgan Chase, Jamie Dimon, noted that the threat of cybersecurity may very well be the biggest threat to the U.S. financial system writ large.

For the fourth year in a row, in 2019, IBM assessed that the financial insurance sector was the most targeted sector in our economy, with 17 percent of all attacks at the top 10 most attacked industries.

The DNI, in January 2019, noted the attacks from North Korea, estimating almost \$1.1 billion in worldwide theft of resources from the financial sector, including \$81 million from the New York Federal Reserve account of Bangladesh's central bank.

And yet, given that significant threat already facing the financial sector, we have seen a dramatic increase in financial sector threats since the COVID pandemic began. In fact, the FBI and the U.K.'s National Cybersecurity Center noted that they are seeing criminal activities on a scale likely to dwarf anything seen before, taking place at a speed that is breathtaking, with a sheer variety of fraud that is shocking.

These are very serious threats. Carbon Black, the company that Tom represents, saw ransomware attacks increase 148 percent in March 2020 over the baseline from just the prior month. And the financial sector was the single largest target of those increases in ransomware attacks, with a 38 percent increase in attacks.

We have seen attacks in Washington State, where the unemployment system has lost hundreds of millions of dollars in the post-COVID environment.

And it isn't just here in the United States. In Germany, the state of North Rhine-Westphalia lost between \$35 million to \$110 million in fraudulent payments based on 3,000 fake requests in the post-COVID environment.

We have seen reports coming out of many government agencies, including the FBI, as well as CISA and other agencies, and we have noted that it isn't simply an attack limited to the United States. We have seen North Korea go around the world.

And what was at one point \$1 billion, in the DNI's testimony, back in January 2019, by the end of 2019 had become \$2 billion, nearly a doubling of their financial sector targeting effects. And they are doing more currently, as we speak.

And it is not just not North Korea. We see China and Russia active in this space. And we see other actors, as Tom Kellermann mentioned, the actors that are nonstate actors, including potential terrorist and extremist groups, taking advantage of the weaknesses in our money laundering systems and the like to exploit our systems to engage in both financial fraud as well as movement of illicit funds.

This is a critical issue that we must confront. And as this committee, I think there are five things that you ought to consider.

First, Juan Zarate, and members of this committee, have suggested that the Secret Service ought be moved back from DHS to the Treasury Department. I think this is a positive move and would help the Secret Service retain its role in cybersecurity.

Second, I think this committee ought to consider offering the Treasury Department an operational role in cybersecurity, giving them the resources and the capability to engage directly with the

financial sector and with the intelligence community that they are already a part of to gather information, send it back out to the community, and bring both the public and private sectors together in this critical industry.

Third, it is important that the committee consider working with the Treasury Department and other departments and agencies to create what the Cyberspace Solarium Commission recommended: a joint collaborative environment where industry and the government could come together in real-time to share threats and to actually collaborate on those threats, not just information-sharing but actual real-time collaboration.

Finally, the committee ought to consider working with Treasury and encouraging them to launch efforts with key allies, as Juan has suggested, to recreate in the G-7 things like the Financial Action Task Force in the anti-money-laundering (AML) arena. AML is a critical issue in this environment where tremendous amounts of money are being sent around by governments and the like, and it is critical that we take action now to address the AML concerns.

And finally, it is important that our government work closely with NATO to expand out our efforts to protect our allies in Europe and elsewhere around the globe.

Thank you very much, and I look forward to your questions.

[The prepared statement of Mr. Jaffer can be found on page 41 of the appendix.]

Chairman CLEAVER. Thank you, Mr. Jaffer.

That is the conclusion of our witnesses' statements. I now recognize myself for 5 minutes for questions.

I would like to spend just a little time talking about the sheer volume of Americans who find themselves teleworking, and the threat that poses to the financial system.

As I mentioned earlier in my opening statement, one-third of the world's populations were in lockdown, and up to 90 percent of financial services employees, banking and insurance companies, were working from home.

We started our conversation today, but earlier, we had a roundtable where we talked about network security. And I believe it was Mr. Kellermann who said that financial institutions have had the best security in the world.

But teleworking and Russian dark web customized malware has allowed adversaries to leverage ways around network defenses. You noted something that I thought was interesting, and I think we sought to address in the COUNTER Act, which is the need for both firms and regulators to be innovative in the way they confront these new fintech criminal techniques.

Mr. Kellermann, and Mr. Coleman, can you both talk a bit about how financial institutions can improve the way in which we can go after these financial criminals and stop these breaches?

Mr. KELLERMANN. Thank you. I would be happy to address that.

First and foremost, we need the defensive line set at the top. The chief information security officers of the financial institutions have been marginalized for too long, and their perspective and their stratagems are not being enacted fully as they compete for resources with chief information officers (CIOs).

Second, I think more proactive cyber threat hunting must occur not only within financial sector participants but across the information supply chain and extend to shared service providers. Cyber threat hunting is much like you need to make sure no one is in the bank vault when you close the doors for the day, not just conducting vulnerability assessments to see if the locks are working or the alarms are working.

And then lastly, because of telework, the major security provisions that have been but in place by banks are no longer effective because the network security paradigm can be bypassed by those VPN tunnels that allow access to those systems. So, I think better forms of authentication and just-in-time administration should be granted within those ecosystems as well.

Chairman CLEAVER. Thank you.

I have a question for Mr. Coleman, but let me just follow up, Mr. Kellerman. You know that all of the members on this committee live in communities. And I am wondering, what do you suggest we do? We have many, many, many banks in our communities. We have all kinds of financial institutions. How do we get to them to implement some of the things that you are presenting to us today? They are not going to participate in our hearings, but they are struggling. What can we do nationally to deal with this issue?

Mr. KELLERMANN. I think that we can incent them through tax incentives for investment in cybersecurity as well as inspire the regulators, whether they be State regulators or national regulators of the Federal Financial Institutions Examination Council (FFIEC), to incorporate this construct of cyber threat hunting. Because with cyber threat hunting, it eliminates the veil of plausible deniability that you may or may not have a problem.

When you conduct a cyber threat hunt, and you identify a bad actor inside your network, it is something that must be acted on immediately. And so, it really provides game day film on what the priority should be in the near term.

Chairman CLEAVER. Thank you. Mr. Coleman, what can we do, what can businesses and educational institutions do to protect themselves and those they serve?

Mr. COLEMAN. Mr. Chairman, our friends at Proofpoint have said to me that defenders don't focus on people but attackers do, meaning 90 percent-plus of effective breaches come through to an end user or to a person. So those breaches that happen, 90 percent of them are because of some human action or behavior. But only about 20 percent, a little less than 20 percent of training dollars, awareness dollars actually go to that end user.

I think we need to flip that. I think we need to encourage businesses to put more investment into their training and awareness. The way we do with, unfortunately, active shooter training or inclement weather training, these other trainings that we have, we absolutely need to do that with cybersecurity as well.

Not so ironically, Americans are hit every single day with these attacks and breaches. Yet, many of them, particularly in the business community, are only getting training once, maybe twice a year.

At the National Cyber Security Alliance, we are encouraging people to perhaps get to the gold standard of once-a-month training

and awareness as it relates to cybersecurity because the threats are evolving so quickly, and we need to be able to educate those folks.

Chairman CLEAVER. Thank you, Mr. Coleman. I appreciate that.

My time is up, so I will now recognize the distinguished ranking member of the subcommittee, Mr. Hill, for 5 minutes for questions.

Mr. HILL. I want to thank the chairman for the hearing. I appreciate our excellent witnesses.

Let me start with Mr. Kellermann. Thanks for coming to the roundtable a few days ago. I wanted to follow up. We talked a little bit about coordination with the regulators at that roundtable. But you made a comment in your testimony today that I thought was interesting about lack of security among fintechs. You used the words, “operational risk.”

Could you get more specific? Are you talking about their AML/BSA compliance on their platforms? Are you talking about their lack of use of APIs? Give me a little color context on your concern about fintech applications.

Mr. KELLERMANN. Whereas, fintechs are the tip of the spear vis-a-vis technological renaissance occurring in the financial sector, we at VMWare Carbon Black have noted increased attacks against the APIs of fintech vendors to bypass security controls they have in place and to leverage what is called island hopping, which is where they attempt to take over the digital infrastructure that was built by that vendor and then use it to attack those who implicitly trust it.

This “island hopping” phenomenon is my biggest concern in this sector, is that you have these entities who are being targeted by very professional cybercriminal crews, typically Eastern European or Brazilian in nature, and they are using the financial platforms that have been developed for greater liquidity and access to financial services and the like to target their constituencies. And so, greater attention must be paid to the security and modernizing the security of fintech participants.

Mr. HILL. Thank you.

Mr. Jaffer, thank you for your testimony, and I appreciate your discussing in your detailed testimony about China and China’s threat, that in March of 2020 a Chinese hacking group carried out one of the broadest campaigns by a Chinese cyber espionage actor that we have observed in recent years.

Mr. Jaffer, are you concerned that China is a new and expanded threat in the cyber arena? In the past, we have frequently talked about North Korea, Iran, and Russia—Eastern European players, as we just noted. How do you think China compares to other countries when it comes to cyber attacks?

Mr. JAFFER. Thank you, Congressman Hill.

China is in the top rank of countries, if not number one of three, along with us and Russia, in terms of cyber capabilities.

Now, the thing about China is they have long been focused on intellectual property theft. They have engaged in what my boss, the former Director of NSA, General Keith Alexander, called the greatest transfer of wealth in human history, literally extracting information out of the United States that they take back to China in

order to repurpose for the purpose of creating economic benefits to their nation. That has been a huge issue.

China is increasingly now pivoting beyond that to intelligence collection, which they have always also done, and they are now increasingly getting involved in financial fraud schemes and allowing these things to take place within their infrastructure.

China doesn't operate only through their government agents, although they have a tremendous number of military intelligence resources devoted to focusing on the United States. They also operate through allowing hackers in their country to take action against the United States and against other allies of ours.

The key issue that we see with China today, though, is what they are doing in terms of covert and overt misinformation and disinformation. They have taken a page right out of the Russians' playbook from 2016, and they are doubling down on that.

We have seen the Chinese Foreign Ministry already talk about the Black Lives Matter movement. It is no accident that the Chinese are talking about that publicly. They are already putting a million of their own people in prisons in the Xinjiang province, and yet they are concerned about Americans.

The reality is, they are not concerned about Americans. What they are concerned about is taking over a global leadership role from the United States, and they will use every means at their disposal to do it, including cyber activities, and that is what makes them particularly dangerous in this arena.

Mr. HILL. Thank you.

Do you see coordination between North Korea and their efforts in cyber attacks? Of course, they are some of the most famous with WannaCry of a few years ago and the Cosmos Bank scheme of just a few months, maybe a year or so ago. Do you see North Korea and China at all coordinating their efforts, or do you see North Korea purely on its own?

Mr. JAFFER. I think North Korea generally acts on its own.

Now, that being said, the North Koreans know how much they can get away with without pushing the Chinese over the line. If the North Koreans go too far, whether it is with nuclear weapons testing or cyber activities or the like, the Chinese will get concerned and potentially take action.

North Korea has gotten smart. They have learned to play the Russians and the Chinese offense against one another too. So they are not simply relying on China as their only client superpower. They are also playing with the Russians.

They have, as you have noticed, though, been fairly quiet when it comes to their testing of nuclear weapons and missiles recently and they have really been focused on the financial gain they can achieve in the current environment. So that is the big concern today for North Korea, although you can't put away the North Korean nuclear problem, which is ever present.

Mr. HILL. Thank you so much.

I yield back, Mr. Chairman.

Chairman CLEAVER. Thank you.

I now recognize Mr. Perlmutter from Colorado for 5 minutes.

Mr. PERLMUTTER. Thank you, Mr. Chairman.

This question is for Mr. Kellermann. A couple of years ago, I had a bill called the Data Breach Insurance Act. And you mentioned tax incentives to try to get companies and individuals to beef up their cybersecurity. Can you discuss that a little bit more, how you see incentives might work to drive folks to the NIST protocol?

Mr. KELLERMANN. Yes. Thank you for asking me that.

I am a huge fan of using that carrot to motivate businesses to view cybersecurity as a functionality of conducting business in today's world versus an expense. Whether it is a percentage of their IT budget that is spent on cybersecurity or whether it is compliance with a standard like NIST or even compliance with a standard which isn't quite a standard but a best practice like the CIS Critical Controls, we would be better off than where we are right now.

Frankly, there is insufficient investment and leadership in the private sector as it relates to cybersecurity, which is why we are dealing with this cybercrime wave.

Mr. PERLMUTTER. Has that been exaggerated, exacerbated, because we are now sort of in this remote telecommuting world? Would we be better off if we were—if smaller companies and small financial institutions were to beef up their cybersecurity?

Mr. KELLERMANN. Yes, it has been exacerbated because of telework. The security of teleworkers is far less than that of someone who is working in a corporate environment because they don't have all the perimeter defenses, much like a corporate facility has greater security than your home typically.

I do think it is an imperative for those organizations to invest more seriously in cybersecurity, but I also realize they are small businesses and they have been dramatically impacted by the economic recession that they are facing.

But going forward, I think most people need to appreciate that encryption is not the sole answer, that encryption is not bullet-proof, it is not something that hackers can't get around. When a hacker hacks your computer metaphorically, they steal the key to unlock the encryption. So what does the encryption really mean? But I will leave that there.

Mr. PERLMUTTER. Okay. I think I may have to dust off the Data Breach Insurance Act and resubmit it over the next month or two to try to use at least some incentive bases so that they can beef it up, knowing full well that a bank robber, no matter how thick the vault is, will always try to find a way to get through that front door, back door, whatever.

Let me change the subject quickly to all of the panelists. Mr. Jaffer was speaking about disinformation. And I am curious if you all have seen efforts, whether it is Black Lives Matter or vaccines or whatever it might be, given the fact we are in this COVID-19 time in history, whether you have seen disinformation campaigns rise.

And I will start—Mr. Kellermann, you are on my screen, so let's start with you, and then go to Mr. Jaffer.

Mr. KELLERMANN. I think that our traditional Cold War adversaries are taking advantage of the situation. The American hegemony, the American empire you might want to call it, is the weakest we have ever been through a combination of factors.

I explicitly don't see true evidence. I am not actually looking for it, because I assume it is happening, frankly, but I do see escalated cyber attack capabilities and activity occurring not just against the financial sector, but against the healthcare sector and a myriad of other sectors in this regard.

Mr. PERLMUTTER. Mr. Jaffer, any comments?

Mr. JAFFER. Yes. Thank you, Congressman Perlmutter.

Yes, we know unquestionably that China has engaged in these type of activities in Taiwan and interfered with their election. We know that Russia did it in 2016 to our election.

We haven't seen specific bulletproof evidence, as Mr. Kellermann pointed out, that they are engaged in those covert activities today when it comes to trying to throw gas on the fires that are already burning in this country. But we know for a fact that they are out there saying it publicly. We see overt activities by the Chinese and the Russians trying to meddle with our political environment.

It is almost unquestionable that when they engage in those type of overt activities, they are doing the same thing covertly.

So, I think that over the next few weeks and months, and probably over the next year, we will see the intelligence community and the Bureau and the rest of our national security organizations coming out with evidence to demonstrate that, in fact, the Chinese, the Russians, and potentially the Iranians are seeking to actively gaslight what is taking place in this country, very real and honest debates are happening, and attempting to manipulate those, let's call it additional chaos and disorder in this country, in the context of the already ongoing pandemic.

Mr. PERLMUTTER. Thank you for that sobering testimony in an already difficult time.

I thank the panelists. Thanks for being part of the roundtable, and today's hearing. And I yield back to the Chair.

Chairman CLEAVER. Thank you, Mr. Perlmutter.

The Chair now recognizes the gentleman from the great State of Texas, Mr. Williams.

Mr. WILLIAMS. Thank you, Mr. Chairman, for calling this hearing.

And thanks to all of you for joining us in this virtual setting for this important hearing.

As cyber criminals get more advanced, we need to make sure our government's efforts to combat these threats are being used as effectively as possible.

Last week, I introduced a bill with my buddy on the other side of the aisle, Denny Heck, to transfer the Secret Service from the Department of Homeland Security back to the Treasury Department, as we have talked about today, where it had previously been located almost 140 years before the September 11th terrorist attacks. This strategic realignment would help put increased focus on the financial crimes and cybercrimes of the Secret Service.

Juan Zarate, the first Assistant Secretary of the Treasury for Terrorist Financing and Financial Crimes after 9/11, and Tim Maurer, author of the book, "Cyber Mercenaries: The State, Hackers, and Power," wrote in a recent op-ed that the move would strengthen the government's ability to protect the financial system

and build on the Trump Administration's interagency focus on cyber threats.

This transfer is also supported by the Treasury Department, by the Department of Homeland Security (DHS), and by the Federal Law Enforcement Officers Association, which advocates for the Federal law enforcement community.

So, Mr. Jaffer, could you give us your thoughts on how this move would be beneficial to our government's ability to defend against financial crimes?

Mr. JAFFER. Absolutely. Congressman Williams, as you well know, the Secret Service was originally set up by Abraham Lincoln in the aftermath of the Civil War in order to protect the U.S. currency. Its first and primary mission was financial crimes.

So, the idea that the Secret Service ought to be focused on that as a primary mission and be in the place where that is the primary role of the agency makes a lot of sense.

I support moving the Secret Service from DHS back to Treasury, in part because it will then prioritize its relationships, existing relationships that Treasury already has in the cyber arena with industry today. And those are very trusted, strong relationships. The Secret Service can build on these.

But I think the Secret Service needs more than that. It is not just a matter, Congressman, of moving them from one agency to another. That is critically important. I think it will elevate their role. But I think it is also about providing them the resources they need to do that job, and do that job better, and to provide them additional authorities, investigative authorities, to really go after this crime.

The Secret Service is largely bound by the authorities they have had historically for a long time, and those are very useful authorities, but there is no question they will need additional resources in this effort.

And being hidden in the larger entity that is DHS makes it harder for them to get priority, harder for them to get resources, and ends up making them focus on their protective mission, which at the end of the day isn't their highest and best value today when it comes to threats facing our financial sector.

So, I support that effort. Juan is a good friend and mentor, and I am glad, Congressman, that you and Mr. Heck introduced that legislation.

Mr. WILLIAMS. Thank you. We will put you on the winning team then, okay?

Mr. JAFFER. Yes, sir.

Mr. WILLIAMS. From hostile countries like China and Russia to other criminals in the private sector, there will always be people looking to exploit our country's cyber vulnerabilities.

In 2018, the Trump Administration put out the updated—the National Cyber Strategy for the first time in 15 years. I applaud this action by the Administration, but I am sure that the threats facing the country are drastically different now than just 2 years ago.

So, again, Mr. Jaffer, would you support mandating this report be updated annually? And can you discuss how the threats facing

government entities and the private sector have evolved over the past 2 years?

Mr. WILLIAMS. Absolutely. Congressman, as you know, the idea that we didn't update our national cybersecurity strategy for a decade and a half is shocking and concerning, and I am glad the President and his team decided to put out a new strategy.

I do think it is valuable for Congress to require the Administration to issue the strategy on a regular basis. Whether that is a year or every 2 or 3 years, I would leave that to you all and the White House to figure out what the right cadence is. But I think it does make sense to have it updated rapidly, because obviously, we are in a constantly changing threat environment.

Now, in particular in the United States today, the threat has changed. You have seen what has already happened. You have heard testimony today about the way that criminals who are very innovative and nation-states who are very innovative take advantage of the current moment. They are not worried about the fact the pandemic is hurting them. They are focused on how to come after us and our people and our finances, and they are very focused on that.

At the end of the day, though, the government's traditional role has been protecting the nation when it comes to all other things from nation-states. But in cybersecurity, we actually have the private sector on the front lines.

So I think Kelvin is exactly right, that this is all about partnerships. We have to bring the government and industry together. And that is why having an entity at Treasury, having Secret Service there, but also giving them operational capability, will help better defend the financial sector where they are on the front line defending today, when normally it would be our military or our law enforcement efforts at the front line.

Mr. WILLIAMS. Okay. Quickly, COVID-19 has given cyber criminals a new opportunity to exploit the crisis to take advantage of hardworking Americans. Many companies and governments have been forced to switch their operations to a virtual setting to conduct their normal operations, just as we are doing right now with this hearing.

So, Mr. Coleman, quickly, what advice would you give companies adapting to these remote settings on how they can stay safe while they are figuring out these new operating procedures?

Mr. COLEMAN. Congressman, I would absolutely advise them, do not abandon your training and awareness. That is a low-hanging-fruit opportunity for them to make sure that their workers are continuing to be resilient in terms of trying to protect themselves. So, the first thing I would say is, please do not abandon the training and awareness that they probably had set up pre-COVID-19.

Mr. WILLIAMS. Thank you, Mr. Chairman. I yield back.

Chairman CLEAVER. Thank you.

The Chair now recognizes the gentleman from Washington, Mr. Heck.

Mr. HECK. Thank you, Mr. Chairman, and Ranking Member Hill. And thank you to all of the panelists. What a spectacular and timely topic for us to discuss.

As the Chair indicated, I represent Washington State, and tragically, unfortunately, nobody has been hit harder by the unemployment insurance fraud that has gone on in this country than Washington State, perpetuated by the cybercrime group that is based in Nigeria, known as Scattered Canary.

We don't know exactly how much they bilked us out of, but we know for sure that somewhere between \$550 million and \$650 million was fraudulently paid out by our State Department of Employment Security. Fortunately, we have been able to recover about \$330 million of whatever the total number is.

And that operation, that recovery was only made possible, frankly, because the U.S. Secret Service was able to identify this operation and went to work. And frankly, I want to express publicly my appreciation to the Secret Service for this on behalf of the taxpayers of Washington State and all Americans for that matter.

But I am not under any illusion that it is just Scattered Canary out there. They are part of one of who knows how many hundreds or thousands of organizations who basically are intent on fraudulently appropriating our money. And that is why I am so concerned. I am very concerned.

Between the lasting damage done to the government's investigative capacity by the Budget Control Act—and it has been diminished—and the loss of mission focus that has been referred to here resulting from moving the Secret Service to the Department of Homeland Security, I think our Federal Government remains pretty unprepared, by and large, to identify and investigate financial cybercrimes, especially factoring in the massive amounts of Federal resources being distributed across the country.

And that is why I was indeed proud to join with my friend, Representative Williams, in introducing the bipartisan and now bicameral U.S. Secret Service Mission Improvement and Realignment Act, which would, of course, as indicated, move the Secret Service back from the Department of Homeland Security to its ancestral home at Treasury.

I think, as has been indicated, that will enable it to tap into the institutional knowledge and expertise at Treasury to better defend us against countering fraud and cybercriminal activity.

So, Mr. Kellermann, I want to ask you the question that Mr. Williams asked of Mr. Jaffer. You specifically mentioned the importance of passing the Secret Service Mission Improvement and Realignment Act. Thank you for that. But I want to ask you, in your own words, why do you think it is important, above and beyond what has been indicated?

And perhaps secondarily, what do we have to lose if we continue to keep the Secret Service housed at the Department of Homeland Security? That is for you, Mr. Kellermann.

Mr. KELLERMANN. Thank you.

I have always been impressed, in my 20 years in cybersecurity, with the efforts of the Criminal Investigative Division (CID) of the Secret Service. They haven't been too flashy and taken too much credit for their successes, but they have done Herculean efforts as it relates to disrupting some of the most advanced cybercrime conspiracies in the world, beginning with the Eastern Europeans' cybercriminal syndicates back in the early 2000s.

But they have always been underresourced, and they have always been stuck in this position where some of their very best analysts had to still provide for protection duty, which put a strain on even then keeping the best technological talent within their ranks.

And this was compounded when they moved over to DHS post-9/11. I understand why, but, at the same time, I think they could truly help us move the needle as it relates to civilizing American cyberspace and thwarting and suppressing some of the more advanced financial crime, cybercrime conspiracies that are ongoing if they were back in Treasury working hand-in-hand with FinCEN and others.

So, again, I tip my hat to you. I think this is incredibly important legislation, and hopefully, it happens.

Mr. HECK. Thank you.

What other steps do you think need to be taken to fill or expand or make appropriate to the measure of the challenge our government's capacity to investigate and pursue financial cybercrimes? Aside from just changing the organizational chart, Mr. Kellermann, what else do we need to do?

Mr. KELLERMANN. I feel that they should be given the resources to hire more personnel, number one.

Number two, they should expand the Electronic Crimes Task Forces—or I think they are now called the Cyber Fraud Task Forces—internationally to get greater information sharing and partnership with various countries who have very significant and very powerful organized crime syndicates who have adopted this cybercrime model.

And then, lastly, when they come across an investigation where there is a cybercrime conspiracy and it is obvious there has been misuse of virtual currencies and alternative payment systems, those moneys could be used to fund their endeavors or fund the efforts to protect the financial sector from attack.

Mr. HECK. Thank you, Mr. Kellermann.

And just finally then, let me say that if Washington State's experience is any measure of this, where in this one instance we have lost hundreds of millions of dollars in just one State, what we are talking about here is a proposition of risk that is billions upon billions upon billions.

I am pleased to have joined Mr. Williams in introducing this bill.

Thank you, Mr. Chairman, and I yield back.

Chairman CLEAVER. Thank you, Mr. Heck.

The Chair now recognizes Representative Gonzalez from Ohio.

Mr. GONZALEZ OF OHIO. Thank you, Mr. Chairman.

And thank you to our witnesses.

Echoing Mr. Heck's comments, this has been an incredibly enlightening and important hearing today. So, I thank the chairman for his leadership and for our witnesses today.

I want to focus my questions primarily on Mr. Kellermann, if you would humor me here. I want to first focus on the attribution issue and our ability to attribute these crimes to different folks.

In both your written testimony and in your oral statement, you talked about how cybercriminals are evolving in both attack sophistication and organization.

Can you shed some light specifically on the organization side? How have cybercriminals evolved, call it, in the last 2 to 3 years, and what are you seeing as sort of the next phase here?

Mr. KELLERMANN. Thank you for the opportunity.

I would cite the World Economic Forum report that there has been an industrialization stage occurring within the economy of scale of the dark web. There are more groups providing specific services and capability sets. You are seeing advanced business models specific to things like access mining.

Access mining is, as a construct, a report issued by VMware Carbon Black over a year ago where hackers will hack systems. If they don't really have a use for those systems, they will profile that system, and they will say, this is Bank A's system. They will then sell access to that system to a traditional criminal, who would have the capacity to liquidate that experience, per se.

In many countries, as we well know, you see this Robin Hood experience where the best cybercriminals are insulated and protected as long as they don't hack anything within those sovereign boundaries and as long as they act in a patriotic fashion. I am sure my friends in the Secret Service or in the FBI can attest to that. But I would say that it is a true economy of scale now, sir.

Mr. GONZALEZ OF OHIO. Is there any sense that these are connected to nation-states, in particular the Chinas and Russias of the world? How directly are the links to some of our adversaries?

Mr. KELLERMANN. From my gut, I feel like there is a link between some of these groups, but, then again, I can't verify that. I am sure that if you had the Secret Service or the FBI testify, maybe in a classified setting, they could speak to that.

I think there is a big difference between, let's say, a Russian hacker and a Chinese hacker. Chinese hackers are less likely to target the financial sector because, frankly, we are their number one debtor, and, frankly, we are their number one consumer. That being said, I don't think it is the case when it comes to Russian-speaking hackers in Eastern Europe.

Mr. GONZALEZ OF OHIO. Right.

And then you also talk about a dark wallet as a platform where jihadists can avoid your customer regulations and launder money.

My question is, technologically, do we have the ability to shut down something like a dark wallet? Is that technologically possible?

Mr. KELLERMANN. I wouldn't be an advocate of, let's say, shutting it down. I would just challenge the developers of these platforms to at least, when called upon, to know who your customer is when called upon, and to be able to freeze the assets associated with anything that has been proven to be part of a criminal or terrorist conspiracy using cyberspace.

I think the FBI, the Secret Service, and the intelligence communities do have the capacity to do more interesting things, but, then again, I am just a watcher on the wall, sir. I don't have that much expertise vis-a-vis dark wallets.

Mr. GONZALEZ OF OHIO. Okay. But your gut is that we do have the capability of being more aggressive with respect to how we go after these individuals or we monitor, to be specific.

With my last minute, another thing you talk about is the international e-forfeiture fund, which I think is really interesting and probably something I want to investigate with you maybe offline when we have more time.

But, just with the minute that I have left, structurally, how would you envision that being set up? Who would be a part of it? And how would it sort of be managed?

And I know that is a lot for 50 seconds, but give it your best shot.

Mr. KELLERMANN. We need to incent developing countries to play ball with us. As we both know, and as most—all of us know for that matter, the most significant entities, transnational organizations and organized crime syndicates within these sovereign boundaries of those countries, don't necessarily have to play ball, and they are just as powerful as the government.

So how do you incent the government to play ball? I think by giving them a percentage of the forfeited assets associated with the investigation. That is why I open it up to an international lens, because most of cybercrime emanates from outside of the United States.

I think probably the Bank of International Settlements might be well-suited to do this, because they already facilitate so much in our financial sector between the tier 1 financials.

Mr. GONZALEZ OF OHIO. Great. Thank you for your insight. We will reach out after this for more depth.

Thank you, Mr. Chairman. I yield back.

Chairman CLEAVER. Thank you.

The Chair now recognizes the gentleman from California, Mr. Sherman.

Mr. SHERMAN. Thank you, and thanks for putting on this virtual hearing.

My first question is for Mr. Kellermann. Included as one of the subjects of today's hearing is a bill that I introduced, the Internet Fraud Prevention Act, which addresses the issue of business email compromise and especially real estate wire fraud.

And the way it typically works in a real estate situation is, you are dealing with somebody who saved their money to buy a house. This would be the one time in their life that they actually send \$50,000 or \$100,000 somewhere. And you hack their email account, know that they are, in fact, buying a house, and you convince them that when they are supposed to wire that downpayment, it is supposed to go to account number "12345" in order to get to their escrow agent, when, in fact, the escrow agent or the attorney involved has a different account number.

And the reason this occurs is when you are supposed to wire money in this country, you only wire it to a number and not to the name of the entity that you are trying to send the money to.

In the U.K., they are implementing a payee matching system where, when you wire money, you are going to wire it to an account number that has to be in the name of whom you actually intend to get the money, and the U.K. regulator believes this will reduce this kind of fraud by 90 percent.

My bill would require the Federal Reserve to perform a cost-benefit analysis for implementing a similar program in the United

States. Would you agree that this is a good approach in order to focus on this issue and prevent people from wiring money to the wrong account?

Mr. KELLERMANN. I do. I do think that it necessitates a cost-benefit analysis. But that being said, any obstacle that we can put in the way of a fraudster is an obstacle worth having.

My mom is a real estate agent, so I hear about this a lot.

Mr. SHERMAN. Thank you.

Ms. Senn, the next one is for you. I am the Chair of our Investor Protection, Entrepreneurship, and Capital Markets Subcommittee, as my colleagues know, and I am concerned about the threat of cryptocurrency-based fraud.

In 2019, just a few months ago, in December, the NASAA identified cryptocurrency as one of the top 5 threats to investors in 2020. Today in your testimony, you note that among the schemes being identified by your organization, this COVID-19 Enforcement Task Force, many involve cryptocurrency or promote investments that are outside the stock market.

The SEC has resisted identifying cryptocurrencies, at least Bitcoin and Ethereum, as securities, and so they say, "Hey, it is not our business, it is not a security, we have an 'S' in our name, that stands for security," and of course they apply the Howey test, I believe that a lack of an SEC registration requirement makes cryptocurrencies attractive to those who have investment scams.

What do you think Congress can do, and what can the States do to correct this system where, if investors want to invest in a real company that really is providing jobs, they have the protection of the SEC and the State commissioners as well, but, for cryptocurrency, they don't get much protection?

Ms. SENN. Thank you, Congressman Sherman.

We do have a regulatory framework in place under the Howey test to regulate investments in cryptocurrency. And on a State level and through NASAA, back in 2018, we initiated a cryptocurrency sweep, and it was a massive public awareness campaign where we notified the public that, hey, guys, these things are out here, they are initial coin offerings, they are investment-related, be aware there are lots of fraudulent offerings, as with any currency as well, but especially in the crypto space, because people don't understand it. Investors are still learning the digital assets if they want to invest properly in that.

But we have a regulatory framework for investment in cryptocurrency. I do believe that, collectively, the States can be more proactive in promoting the types of frauds that are prevalent—

Mr. SHERMAN. If I can interrupt, the SEC clings to this idea that Bitcoin and Ether are not securities, and, therefore, they don't have jurisdiction. Do the State securities commissioners believe they have jurisdiction in those who are selling Bitcoin and Ethereum?

Ms. SENN. If the cryptocurrency is being offered as an investment, or with a view toward an investment—yes, sir. I know.

Mr. SHERMAN. If every—

Ms. SENN. We also have many transmitters laws.

Mr. SHERMAN. Everybody who buys Bitcoin is buying it with the prospect of it going up. Every cryptocurrency enthusiast who hears a rate, and invests in it, believes it is going to go up.

I believe my time has expired, so I yield back.

Ms. SENN. I am in agreement.

Chairman CLEAVER. The Chair now recognizes Representative Rose from Tennessee.

Mr. Rose?

We will move on to Mr. Taylor from Texas.

Mr. TAYLOR. Thank you. I really appreciate you putting this hearing together, and I think it is important information. I am reminded of something that Frederick the Great said long ago: "He who defends everything defends nothing."

Part of the issue here I think in this whole discussion is prioritizing resources. And I have heard a lot about where we need to prioritize resources and not prioritize resources. And I guess something that I have been thinking about is in—and I know there has been a mention of the AML/BSA program that financial institutions pursue in trying to find anti-money-laundering and, with the Bank Secrecy Act, trying to find problems in terms of prioritizing.

I guess I will just kind of ask a broad question: Have you seen people wasting resources, wasting the effort, or they are trying to do the right thing, but they are headed down the wrong path in terms of what they are doing? I will throw that out, just experiences from the field. What have you seen that you think, gosh, that is a waste of time and effort?

Mr. Coleman, do you want to take a crack at that?

Mr. COLEMAN. Congressman, fortunately, I have not experienced that in cybersecurity. Most of the time it is the exact opposite in terms of trying to help people understand the urgency of investing or taking action throughout normal times, let alone a disaster.

Jon Check from Raytheon, whom I work with, often talks about how bad actors will take advantage of a disaster, manmade or natural, a situation like we are in now, Congressman. And so getting companies, businesses, individuals to act during those times is difficult enough, let alone during peacetime.

So, no, I haven't necessarily seen where people are going down the wrong path or wasting time. Actually, it is the opposite in terms of trying to encourage them to go forward.

Mr. TAYLOR. Anybody else want to take a stab at that one and talk about prioritization and making sure resources are being used intelligently?

Mr. JAFFER. Congressman, I think one place that you might look is oftentimes, you see a company go out and buy every tool they can out there. And they put a lot of them on the shelves and they don't utilize them.

So one thing that we can do is really encourage companies to identify the best out there in the field and buy that capability, use that capability. And if you are not going to use it, don't buy it. If you don't have the capacity to take care of it right now, don't invest in it at this time. I think it prioritizes that, and that way is a sensible approach for institutions.

I also want to associate myself with Mr. Kellermann's remarks earlier about providing carrots to industry to take advantage of cybersecurity protection, and so I think that giving tax incentives is the right way to go.

A different approach would be to regulate and to tell people exactly what to do and what not to do. The problem with that in my mind is that it creates a check-box mentality, and in a field where things are changing so rapidly, sir, I think it is a mistake to require the type of regulations that would be very specific and detailed and ultimately cause people to just check the box and not actually gain on security gains.

Mr. TAYLOR. In my own experience, I was on a bank board for 12 years, and we acquired a product which automated the verification of checks that were written fraudulently. And so, by automating that, we were able to reduce resources in that effort and actually be more effective. We actually saw reduction in our fraud at our bank. But we also were then able to put more resources into other counter-fraud efforts.

And so I think making the right investment, as you say, a part of that is knowing where the efficiency is to be gained and then, in turn, understanding where we can actually go get those efficiencies.

And I look forward to working further on this issue. Cybersecurity is increasingly becoming a concern in our country because we are automating more, and the more we automate, the more we turn to systems and computers to do things, the more stuff is on the web, the more vulnerable we become or the more we have to defend it.

With that, Mr. Chairman, I yield back.

Chairman CLEAVER. The gentleman yields back.

The Chair now recognizes the gentleman from New Jersey, Mr. Gottheimer.

Mr. GOTTHEIMER. Thank you so much, Chairman Cleaver and Ranking Member Hill, for calling this hearing, and to all of our witnesses for being here today.

TransUnion, one of the big three credit bureaus, runs a weekly survey that shows that 29 percent of consumers say they have been targets of digital fraud related to COVID-19. On top of that, AARP's Fraud Watch Network recently reported that there has been a steep increase in scams targeting the elderly and other vulnerable communities.

These nefarious actors, both domestic and international, are using the pandemic and preying on people's fragile states in these uncertain times to target their hard-earned retirement accounts, their unemployment checks, and other savings.

Ms. Senn, from your perspective of working directly to prevent cybercrime as the Chair of the Cybersecurity Committee for the NASAA, do you agree that seniors are disproportionately the victims of cybercriminals? And what challenges do law enforcement run into while trying to prevent this population from falling victim to frauds and scams?

Ms. SENN. Thank you, Congressman.

Yes, seniors are disproportionately targeted. They hold most of the nation's wealth. You work your entire life so that in your gold-

en years, you hopefully can sustain the rest of your life with the retirements that you have saved. Criminals know that. That is where the money is.

You have heard the studies where, as you age, your cognitive function declines, and your financial judgment is part of that. And so, seniors are more vulnerable to financial fraud because of that, the weakening in their financial judgment.

Through NASAA, our North American Securities Administrators Association, we have developed a model law to report the suspected financial exploitation of seniors, and, through that law, which 27 States have passed—yesterday was Elder Abuse Awareness Day, and we were pleased to announce that—we have reports coming in. So we can review—I have a stack of them on my desk here of the types of frauds that seniors are being exposed to.

And especially now, during the COVID-19 pandemic, seniors are at home, they are being isolated, they are away from their friends and family who normally check on them to see how things are going and ensure that they are not online surfing the internet and being solicited by fraudsters.

And so, it is critical during this time to reach out to your friends and family, check on them, make sure that things aren't unusual, red flags—I could talk about those all day—but to continue to report suspected financial exploitation.

I want to mention one thing about the financial industry, because we regulate on the State level the small businesses. And I know you guys are talking at a macro level, but on a micro level, we see the trickle down. I sit down with the victim investors and talk with them about the frauds that have impacted them, and some of them have been ripped off of their entire life savings, and it is a problem for all of us—

Mr. GOTTHEIMER. What do you think States—if I could just follow up on that—what do you think States can do, what should we equip States to do to be able to fight back and protect vulnerable populations from fraud? Are there things you would recommend?

Ms. SENN. Congressman, yes. I mentioned in my opening remarks and in my written testimony, we—NASAA supports the Senior Investor Pandemic and Fraud Protection Act, and I believe that is legislation that you are interested in, which would allow States to apply for a grant. And I know we do a great job with the limited resources that we have, but, sir, we can do better.

For example, in Alabama, we are able, through a small grant, to hire a victim service officer to assist our financial abuse victims, mostly seniors, with reporting and to provide that human element. So it is critical, yes—

Mr. GOTTHEIMER. Ma'am, I am glad you mentioned the legislation that I have drafted. The Senior Investor Pandemic and Fraud Protection Act does a lot, I think, that would really help in that effort to allow qualified States to apply for these grants, to be able to hire and train investigative staff, which seems like that would make a difference, whether it is purchasing technology and equipment or developing other materials to fight fraud.

And I am going to ask unanimous consent, Mr. Chairman, to submit a series of letters from industry and consumer groups in support of this draft legislation into the record.

Chairman CLEAVER. Without objection, it is so ordered.

Mr. GOTTHEIMER. Thank you so much.

I can't tell how much time I have left. Mr. Chairman, how much time is that? It is not coming up. How long?

Chairman CLEAVER. One minute.

Mr. GOTTHEIMER. One minute. So I will just say, as the world races to find a cure for COVID, Iranian and Chinese hackers have waged cyber attacks targeting American companies, universities, and research institutions, the pharmaceutical company Gilead Sciences, and the World Health Organization (WHO).

Mr. Jaffer, in the time we have left, how vulnerable is our financial sector to state-sponsored hacking at this time?

Mr. JAFFER. I think state-sponsored hacking is the biggest threat to our financial sector because of the capabilities they can bring to bear.

If you think about what nation-states have, they have almost unlimited resources, both human and monetary, to throw at a problem. So, any single private-sector company, whether it is JPMorgan Chase or a small community bank like you were talking about, they simply don't have the resources to be able to go up against that kind of a threat.

That is why we have to bring them together in a collective defense fabric, one bank with another, large banks with small banks, all coming together collectively to defend one another in this scenario. You just can't beat a nation-state at their own game.

Mr. GOTTHEIMER. Thank you, Mr. Jaffer.

Ms. Senn, thank you for your answers.

And thank you, again, to the chairman and the ranking member and our witnesses. I yield back.

Chairman CLEAVER. Thank you.

The gentleman from Tennessee, Mr. Rose, is now recognized for 5 minutes.

Mr. ROSE. Thank you, Chairman Cleaver and Ranking Member Hill, for yielding and for holding this hearing today.

I also want to thank our witnesses for their testimony and for their expertise.

As the COVID-19 pandemic continues to impact our country, fraudsters and cybercriminals have seized the opportunity to prey on vulnerable Americans. They have exploited this crisis to infiltrate our institutions and are a systemic threat to our financial system.

The number of cybersecurity complaints in the last 4 months has spiked to as many as 4,000 incidents a day.

Ms. Senn, would you please outline to what extent we are seeing an increase? That is, is it exponential, or does it compare to fraud seen in the wake of other natural disasters?

Ms. SENN. Thank you, Congressman.

In my opinion, it is exponential. I can speak from my perspective here in Alabama and for other States that we have seen a dramatic, 50 percent uptick in the number of financial exploitation reports that are coming in during this time.

Like I mentioned earlier, I have a stack of them on my desk, because primarily, seniors are at home alone. The computer is a source of social—it is a social platform. People are online more.

They are ordering food and other items online. Shopping online is a tremendous source of fraud. They are being inundated with pop-up things, and people just don't know how to sort through BS and get to the legitimate sites.

And our brokerage firms, you all mentioned small businesses, a lot of them are working from home. And so, we are working to ensure that controls are in place for the small businesses that we regulate on the financial side.

Mr. ROSE. Thank you.

Cyber threat actors have been taking advantage of the crisis to undermine the U.S. Government, to prod systems for weaknesses, and stoke fear and confusion.

Professor Jaffer, where are a majority of these cyber attacks originating from, and what has been their main target?

Mr. JAFFER. Thank you, Congressman.

Obviously, the vast majority of cyber attacks that come against our country are coming from a combination of nation-states and fraudsters. So it depends on what we are talking about. If we are talking about major attacks on our banking system or the like, we have seen that come from countries like North Korea, and from Iran. We saw the 2016 and the 2012 attacks on our banking system by Iran, and those continue apace.

Our government is targeted by all manner of nation-states and patriotic hackers and the like. I don't really believe in patriotic hackers. Those are simply nation-states acting through proxies.

At end of the day, if we are really going to defend this nation when it comes to cyberspace, we have to realize that we have put the private sector on the front lines unlike any other scenario. We don't expect Target and Walmart to defend against Russian Bear Bombers coming across the horizon, yet today in cyberspace we expect exactly that of JPMorgan, Citibank, Walmart, Target, and every mom-and-pop institution, whether it is a bank or a bakery, to defend against the Russians, the Chinese, and the Iranians. That is simply an unsustainable scenario, and we have to bring the nation together.

Large banks have to protect small banks. Large corporate institutions have to protect other smaller corporations. We have to take a supply chain mentality to this.

And that is something that the government single-handedly can bring together and create that joint collaborative environment that the Cyberspace Solarium Commission talked about in order to make that happen. It requires us to move and act in real time. We can't simply wait and have the conversation a day or two later. By that time, your systems are down, sir.

Mr. ROSE. Picking up there, Professor Jaffer, have we given our law enforcement agencies and the criminal justice system the tools that we need to give them to combat this 21st Century challenge?

Mr. JAFFER. Thank you for that question, Congressman.

We have historically given a lot of the tools that our government needs. One of the challenges we face today, though, is that we have a debate in this country about the right authorities for police, the right authority for our intelligence community. You see the expired provisions of the USA Patriot Act. We are now in a pre-9/11 era

when it comes to protecting ourselves against foreign nation-state threats and terrorist threats.

The same is true of cybercriminals. Those same authorities we used are gone. And the fact that we haven't been able to come together as a country and reauthorize those provisions which are—one of which is controversial, two of which are absolutely non-controversial, is really a concern. And we really have to come together and provide authorities and add authorities, as we are doing with the Secret Service, and resources to really address these threats.

It is a hard thing to do in a time we are spending a lot of money on restarting our economy, but it is something we have to do if we are going to protect it in the long-term, sir.

Mr. ROSE. Quickly, one follow-up question. I have always felt like we probably were not getting to the easiest place to cut off the threat, so the providers of access to the internet. Do you think we have enough and a robust enough set of tools in that arena to combat crime in the cyber era?

Mr. JAFFER. The providers do a lot today to take spam off the network and the like. Could we empower them with more capabilities, more authority, frankly, more information from the government? Absolutely.

The truth is that we have been talking about the government giving classified information to the private sector to defend itself for the better part of almost a decade and a half. We have never really acted in a serious way. That is on the intelligence community on one side. But it is also on industry, because the industry has to show the government where the attack is from.

And so, we have to create that shared situational awareness, but both sides have to play, and the government has to give more classified information to industry and in a form they can actually use it, sir, and that is the most important thing.

It is one thing to pull somebody in a room and say, "Here is a bunch of secrets." Walk out, you can't say anything about it. It is different to give them the actual information and let them use it to defend themselves.

Chairman CLEAVER. Thank you, Mr. Jaffer.

Mr. ROSE. Thank you. I yield back. I think I have ran out of time, but the clock disappeared.

Chairman CLEAVER. Yes. Well, this is your gift for the day.

Mr. ROSE. I yield back.

Chairman CLEAVER. Ms. Wexton of Virginia, you have 5 minutes.

Ms. WEXTON. Thank you, Mr. Chairman.

And thank you to the witnesses for being with us today. This is a really fascinating and obviously a very timely discussion.

One of the pieces of legislation that we are considering today is a bill that I am working on, the COVID-19 Restitution Assistance Fund for Victims of Securities Violations Act, which would create a fund at the SEC to provide restitution payments for individuals harmed by COVID-19-related securities fraud if they don't otherwise receive full restitution.

Ms. Senn, I was pleased to hear you reference this bill in your opening remarks. Do you agree with this approach? Do you think that this is a positive piece of legislation?

Ms. SENN. Overwhelmingly yes, Congresswoman. As a long-time prosecutor, 10 years of financial crime, I have spent many long hours on the topic of victims who will never see another cent of the money that was stolen from them by fraudsters. And, in Alabama, there is not a recovery fund for victims of financial crimes. And so, yes, Alabama and NASAA overwhelmingly support the establishment of this fund.

Ms. WEXTON. And you say in your testimony that victims of investment scams often have a hard time recovering their losses. Can you explain why that is, and what are some of the challenges that they faced in recovering their losses?

Ms. SENN. Yes, ma'am. As my distinguished colleagues on the panel have mentioned several times, that money goes overseas, and we see it in the bank records. We coordinate regularly with our Federal partners. The FBI can provide us with the exact location, but we can't go out and get it.

As Congress is aware, there are certain threshold requirements. Due to the limited resources, we have to allocate them properly. So, we can't go after Ms. Jones' \$50,000 that she put as a down payment on her house. Maybe that came from a brokerage firm. It is just not possible to spend the money to go out and get that. And so, those people oftentimes have seen entire retirement accounts dissipated, and they have nowhere to turn. They don't have friends and family to look after them. So they turn to public welfare, and it is a sad situation. But victims of financial fraud need a recovery fund.

Ms. WEXTON. It is very sad that someone's entire life savings wouldn't be enough to go and recover it as best we can. But do you have any suggestions or thoughts about what other actions Congress can take to uncover and prosecute those who would commit fraud in this way?

Ms. SENN. Yes, ma'am.

As mentioned earlier, the States come together, we coordinate, and we communicate. If there is a fraudster in one State, we have internal communications where we ensure that our resources are being allocated properly so that we can go after these folks.

And we are also coordinating with our Federal counterparts, the SEC, CFTC, FBI, and DOJ. But we all have limited resources. I know, on the State side, particularly with the financial fraud that we are seeing, everybody needs more money for technology.

I am listening to my panelists, and I am shaking my head in agreement, yes, especially the smaller businesses. The cybersecurity protocols 20 years ago were nothing in comparison. You tried to make sure your computer was updated occasionally. And so, it is overwhelming to small businesses across the State, so I mention those things, money as always.

Ms. WEXTON. Great. Thank you so much, to all of you. With that, I will yield back, Mr. Chairman.

Ms. SENN. Thank you.

Chairman CLEAVER. The gentlelady yields back.

The Chair now recognizes Mr. Lynch from Massachusetts.

Mr. LYNCH. Thank you, Mr. Chairman. First of all, I want to thank you, Mr. Chairman, for holding this hearing, and also Rank-

ing Member Hill. I want to thank our witnesses. They have all been terrific, and I really appreciate their testimony.

Mr. Chairman, I don't have many more questions, but I sort of handle a similar topic over on the House Oversight and Reform Committee, where I chair the Subcommittee on National Security, and we sort of overlap. And one of the earlier questions was what evidence do you have as to the nature of some of these cyber intrusions.

So, we have submitted a request to our intelligence agencies to do a classified briefing when we get back into D.C. And I was wondering if, Mr. Chairman, you would cosign that request and we would do a joint classified briefing so that we can get into some of the details of this that we cannot discuss in this forum, which is unclassified?

But that is my one request. And it would be expanded not only to the cyber hacks, but, also, there is evidence that foreign actors are also online, exacerbating and disrupting some of the discussions around us reforming our criminal justice system and the brutal murder of George Floyd in Minneapolis.

They have been piling on, on top of that issue, too, and we would like to drill down and see what actions some of these malign actors overseas, both government-wise but also individual hackers, have influenced that debate as well.

So, that is all I have. I would love to have you join us. I think it is one of the common interests between our committees, and it is also bipartisan. It is shared among our colleagues.

In closing, I do want to say that I fully endorse the Realignment Act that has been put forward by Mr. Heck and Mr. Williams, and I am happy to support that, and I will yield back. Thank you, sir.

Chairman CLEAVER. Thank you, Mr. Lynch. We look forward to working with you to see what—and I would ask Mr. Perlmutter as well, and Ranking Member Hill to sit down with you. I think we should work together on this issue.

The Chair now recognizes the Chair of the Full Committee, the gentlewoman from California, Chairwoman Waters.

Chairwoman WATERS. I would like to thank you for convening this hearing on the cybersecurity threats and electronic fraud issues that have proliferated during the COVID-19 pandemic. Persistent cyber attacks on our financial system are not new. I don't know if you have had this discussion this morning, but I am concerned that some minority communities, and particularly those with higher limited-English-proficient populations, are more vulnerable to predatory practices and scams during the COVID-19 pandemic.

For example, in the last financial crisis, consumer groups reported that borrowers with limited-English-proficiency paid thousands of dollars to scammers for foreclosure prevention help that never materialized, with cybersecurity complaints to the FBI increasing from 1,000 per day to 4,000 daily, which scams have been predominantly targeting seniors, minorities, and individuals with limited English proficiency during this pandemic.

What can financial regulators and advocacy groups do to better protect and educate consumers in these communities against such threats?

I would like to address this to all of our witnesses. Any one of you can start with a response to this if you have any information or advice about what is happening as this fraud is targeted toward these minority communities.

Mr. COLEMAN. Chairwoman Waters, this is Kelvin Coleman with the National Cyber Security Alliance. I will start by saying that with the nation being over 360 million Americans in 50 States and 6 territories, the National Cyber Security Alliance has been very successful in using force multipliers for trusted community groups to spread our message about cybersecurity awareness and education. I think this is the perfect opportunity to do that as well. So, utilizing and speaking with organizations that are trusted and embedded in those communities to carry our message forward, because oftentimes, these are low-hanging-fruit solutions that we can recommend to people.

I know Amanda and Jamil and Tom are talking about some pretty sophisticated products and processes that the U.S. Government can look at. But when it comes to the average citizen, we need to be talking about more basics, like password protection, making sure that they are patching their systems, that they are up-to-date. And so, I would advocate utilizing those existing embedded community groups to really, again, use them as our force multiplier to get the message out there to them.

Chairwoman WATERS. Ms. Senn?

Ms. SENN. Chairwoman Waters, I will add to Kelvin's comment that the States—we have discussed this—have provided translators in the communities in some of our States, because they know the communities, our State securities regulators understand their communities' needs, and they are able to partner with private industry to host workshops and investor education events and have folks there to translate.

Chairwoman WATERS. Thank you very much for that response.

And I just want to say to the chairman, I thank you so very much. This is a subject that is going to get a lot of attention based on our new normal. So, thank you very much.

I yield back the balance of my time.

Chairman CLEAVER. Thank you, Madam Chairwoman.

Let me, at this time, thank all of the witnesses for their very helpful, insightful testimony.

Without objection, I would like to offer letters of support for this hearing provided by the FACT Coalition; the National Association of Federally-Insured Credit Unions; a submission for the record by the Washington, D.C.-based think tank Third Way; and a number of letters of support for legislation to reauthorize and funding the Senior Investor Protection Grant Program.

Without objection, it is so ordered.

The Chair notes that some Members may have additional questions for this panel, which they may wish to submit in writing. Without objection, the hearing record will remain open for 5 legislative days for Members to submit written questions to these witnesses and to place their responses in the record. Also, without objection, Members will have 5 legislative days to submit extraneous materials to the Chair for inclusion in the record.

With that, this hearing is adjourned.

[Whereupon, at 1:44 p.m., the hearing was adjourned.]

A P P E N D I X

June 16, 2020



**TESTIMONY OF
KELVIN COLEMAN - EXECUTIVE DIRECTOR
NATIONAL CYBERSECURITY ALLIANCE**

**BEFORE THE SUBCOMMITTEE ON THE NATIONAL
SECURITY, INTERNATIONAL SECURITY,
INTERNATIONAL DEVELOPMENT AND MONETARY
POLICY**

**“CYBERCRIMINALS AND FRAUDSTERS: HOW BAD
ACTORS ARE EXPLOITING THE FINANCIAL SYSTEM
DURING THE COVID-19 PANDEMIC” EXAMINING
OPPORTUNITIES FOR FINANCIAL MARKETS IN THE
DIGITAL ERA”**

JUNE 16, 2020

Chairman Cleaver, Ranking Member Hill, and Members of the Committee:

Thank you for inviting me to join today's hearing. It is an honor to be here. My name is Kelvin Coleman. I am the Executive Director and Chief Executive Officer of the National Cyber Security Alliance, an organization comprised of twenty-seven of world's leading companies in technology and cybersecurity.

I am pleased to represent the National Cyber Security Alliance (NCSA) at this important hearing. NCSA's core mission is to build strong public/private partnerships to create and implement broad-reaching education and awareness efforts to empower users at home, work and school. We provide users with the information they need to keep themselves, their organizations, their systems and their sensitive information safe and secure online and encourage a culture of cybersecurity. Simply put, our vision is to empower a more secure, interconnected world.

We work hard every day on this vision because the United States confronts a dangerous combination of known and unknown cyber vulnerabilities. And we have known about these vulnerabilities for quite some time now. Today, we face strong and rapidly expanding adversaries with ever increasing cyber capabilities. We face persistent, unauthorized, and often unattributable intrusions to Federal, State, Local and private sector networks. The products and processes we put into place to mitigate these challenges are certainly part of the solution but I believe we need to focus even more on another aspect: partnerships.

NCSA is the proven public/private partner that focuses industry and government efforts. We do this by: 1) Convening partners who recognize strength in the security collective; 2) Educating individuals on cybersecurity best practices; and 3) Amplifying collective efforts to increase cybersecurity awareness. To accomplish these goals, we rely on a number of programs and partners.

This is especially true during the COVID-19 era. NCSA, our board member companies, federal partners and non-profit collaborators have worked swiftly to provide organizations and individuals with relevant and helpful information to address security and privacy concerns surrounding the global COVID-19 outbreak.

To help individuals and organizations find resources they can use and share, NCSA has launched the **COVID-19 Security Resource Library**. This library features free and updated information on current scams, cyber threats, remote working, disaster relief, and more. NCSA will work diligently to update this page regularly as resources become available. We also created a Covid-19 webinar series for the small and medium size business community. The webinar series focused on teleworking, e-commerce and mobile payment security. The Federal Trade Commission was featured in the series.

One of our primary tools in this effort to educate Americans on threats and solutions related to technology is **Cyber Security Awareness Month (CSAM)**. Led by NCSA, CSAM is held in October and is a collaborative effort between government and industry that raises cybersecurity awareness and ensures that all Americans have the resources they need to be safe and secure online.

Focusing on key areas like privacy, consumer devices, and e-commerce, CSAM emphasizes shared responsibility and personal accountability in cyberspace, stressing the importance of taking proactive steps to enhance cybersecurity at home and in the workplace.

During CSAM, we emphasize the importance of cybersecurity awareness; however, the conversation does not end when October is over. Cybersecurity awareness should consistently be part of conversations with stakeholders, family, friends, and our communities.

Another vehicle NCSA uses to raise awareness is our **Data Privacy Day campaign**. This campaign, led by NCSA, began in the United States and Canada in January 2008 as an extension of the Data Protection Day celebration in Europe. Data Protection Day commemorates the Jan. 28, 1981, signing of Convention 108, the first legally binding international treaty dealing with privacy and data protection. On Jan. 27, 2014, the 113th U.S. Congress adopted [S. Res. 337](#), a non-binding resolution expressing support for the designation of Jan. 28 as “National Data Privacy Day.”

Data Privacy Day is the signature event in a greater privacy awareness and education effort. Year-round, NCSA educates consumers on how they can own their online presence and shows organizations how privacy is good for business. NCSA’s privacy awareness campaign is an essential component of the global online safety, security and privacy movement.

A third program that NCSA uses to build a more secure world is **CyberSecure My Business**. CyberSecure My Business is a national program whose mission is to help small and medium-sized businesses (SMBs) learn to be safer and more secure online. The program offers a series of virtual and in-person, highly interactive and easy-to-understand workshops based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework to educate the SMB community about:

- Identifying and understanding which business assets (“digital crown jewels”) others want
- Learning how to protect those assets
- Detecting when something has gone wrong
- Responding quickly to minimize impact and implement an action plan
- Learning what resources are needed to recover after a breach

Additional components of CyberSecure My Business include: monthly webinars with industry, government and nonprofit cybersecurity experts, online portal of resources to help the SMB community and monthly newsletters summarizing the latest cybersecurity news.

In addition to these programs, NCSA also offers a number of resources that speak to online safety basics, theft/fraud/cybercrime, key accounts and devices security and ways to manage privacy. One of our most popular resources are our toolkit and tip sheets. Updated annually, NCSA toolkit and tip sheets provide a comprehensive guide for individuals and organizations, regardless of size or industry, on engaging in and promoting cybersecurity awareness and developing effective practices that foster strong and lasting cybersecurity. The toolkit and tip sheets offer a variety of ways to get stakeholders engaged in the cybersecurity awareness effort anytime and anywhere.

While these programs and resources provide tremendous value in the fight to protect Americans, I would say our biggest asset can be found in the incredible partnerships we have developed over the years in both the public and private sectors. Chief among those partnerships is the one NCSA shares with its 27 Board member companies.

NCSA's Board is comprised of some of today's leading companies in areas such as cybersecurity, software, social media and consumer services. Board member companies include:

ADP • AIG • American Express • Bank of America • CME Group • Cofense • Comcast • ESET North America • Facebook • Intel Corporation • Lenovo • Eli Lilly • LogMeIn Inc. • Marriott International • Mastercard • MediaPro • Microsoft • Mimecast • KnowBe4 • NortonLifeLock • ProofPoint • Raytheon • Trend Micro • Uber • US Bank • Visa, Inc. • Wells Fargo

NCSA Board member companies are viewed as leaders in cybersecurity education and awareness and are an integral part of making the organization a successful public-private partnership. The Board also provides NCSA with organizational and fiscal oversight.

While the private sector is an incredibly important partner, the Federal Government plays an equally important role in cybersecurity education and awareness. Chief among NCSA's Federal Government partners is the Cybersecurity and Infrastructure Security Agency (CISA).

CISA and NCSA have worked to enhance tools and materials for cybersecurity awareness in a number of ways. Some of these include materials covering topics related to basic cyber hygiene, workforce, Internet of Things, Staying Safe Online During Tax Time (February and March); Digital Spring Cleaning, National Supply Chain Integrity Month (April); National Small Business Week (May); CyberTrip Advisor (June); National Cybersecurity Awareness Month (October); CyberSafe Holiday Shopping, Critical Infrastructure Security and Resilience Month (November) and Digital New Year's Resolutions (December). Other activities with CISA include redesigning the website with improved tools making it easier for consumers and stakeholders to engage in the various campaigns.

CISA and NCSA have worked in tandem to plan the "kick-off" of CSAM events across the nation. To engage diverse geographic areas, CISA & NCSA have coordinated with trusted community partners in CISA's 10 regional locations to encourage hosting CSAM events including facilitated workshops. Every year CISA leadership is invited to participate in the NCSA and Nasdaq Cybersecurity Summit. A signature CSAM initiative, this mediagenic event provides a unique and well-attended forum to discuss the state of cybersecurity.

While CISA is by far NCSA's closest Federal partner, we do engage with a number of other Federal departments and agencies including:

- National Institute of Standards and Technology
- Federal Trade Commission
- Federal Bureau of Investigation
- Small Business Administration
- Federal Trade Commission

- Federal Communication Commission

CONCLUSION

NCSA, in coordination with its many partners at the public and private sector levels, has put a lot of effort into building a more secure, connected world. With that said, there is still so much to be done. Congress should consider making game changing investments in cybersecurity awareness and education. Investments that could benefit the American people as well as the small and medium sized business community. As Americans began to rely more heavily on telework, bad actors will increase their malicious activities and target those working from home. Americans must be equipped with the knowledge to protect themselves and their communities. Congress can and should play an important role in making sure Americans understand the many dangers of inadequately securing their systems, devices and information.

Prepared Statement of Jamil N. Jaffer¹
on
Cybercriminals and Fraudsters: How Bad Actors Are Exploiting
the Financial System During the COVID-19 Pandemic
before the
Subcommittee on National Security, International Development and Monetary Policy
of the
United States House of Representatives Committee on Financial Services

June 16, 2020

I. Introduction

Chairman Cleaver, Ranking Member Hill, and Members of the Subcommittee: thank you for inviting me to discuss the very real cyber threats facing the U.S. financial sector, as well as the global financial system writ large. As you all too well know, these threats are currently targeting key financial institutions in allied nations and have become particularly problematic in the midst of the current pandemic. I hope that we will have the opportunity for a frank discussion about these matters, building on your bipartisan virtual roundtable last month,² and to have a robust discussion about what steps we might take as a nation to defend against these very significant threats.

At the outset, I want to note your leadership, Mr. Chairman, on critical cybersecurity issues, including working to secure our nation's oil and gas pipeline infrastructure,³ highlighting, earlier this year, the very real threat of Iranian cyberattacks against the United States, particularly against American financial institutions,⁴ and your longstanding efforts to fight foreign overt and covert disinformation efforts online, including those that seek to divide us as a nation.⁵ I strongly share your views on the need to address these issues, including ensuring the security of

¹ Jamil N. Jaffer currently serves as Founder & Executive Director of the National Security Institute and as an Assistant Professor of Law and Director, National Security Law & Policy Program at the Antonin Scalia Law School at George Mason University and is affiliated with Stanford University's Center for International Security and Cooperation. Mr. Jaffer also serves as Senior Vice President for Strategy, Partnerships & Corporate Development at IronNet Cybersecurity, a startup technology products company headquartered in the Washington, DC metropolitan area. Among other things, Mr. Jaffer previously served as Chief Counsel & Senior Advisor to the Senate Foreign Relations Committee, Senior Counsel to the House Intelligence Committee, Associate Counsel to President George W. Bush, and Counsel to the Assistant Attorney General for National Security in the U.S. Department of Justice. Mr. Jaffer is testifying before the Committee in his personal and individual capacity and not on behalf of any organization or entity, including but not limited to any current or former employer. Mr. Jaffer would like to thank Jon Hoffman and Taylor Nelson for their excellent research and other assistance in the preparation of this testimony.

² See Press Release, *Committee to Hold Bipartisan Virtual Roundtable with Cybersecurity Experts* (May 28, 2020), available online at <<https://financialservices.house.gov/news/documentquery.aspx?IssueID=126804>>.

³ See H.R. 3699, *Pipeline Security Act*, available online at <<https://www.congress.gov/bills/116th-congress/house-bill/3699>>.

⁴ See, e.g., Rep. Emanuel Cleaver, II & Rep. Gregory Meeks, *Letter to Treasury Sec. Steve Mnuchin* (Jan. 7, 2020), available online at <<https://cleaver.house.gov/sites/cleaver.house.gov/files/iran%20Cyber%20Risks%20Letter.pdf>>.

⁵ See, e.g., Rep. Bonnie Watson Coleman & Rep. Emanuel Cleaver, II, *Letter to Twitter CEO Jack Dorsey* (Oct. 3, 2017), available online at <<https://cleaver.house.gov/sites/cleaver.house.gov/files/Ltr%20to%20Twitter%20CEO.pdf>>.

our energy infrastructure,⁶ responding strongly to Iranian cyber aggression,⁷ and combatting foreign efforts to create chaos and division within our society.⁸ I also share a personal interest in your efforts to increase diversity in the technology sector, as well as in the national security arena, an increasingly important area to focus on as we seek to move forward as a nation in light of recent events.⁹

Likewise, I want to highlight Ranking Member Hill's strong and consistent advocacy and leadership on these matters also, such as protecting Americans against identity theft,¹⁰ imposing stiff sanctions against Russia for its meddling in the 2016 elections,¹¹ pressing NATO to extend its security umbrella to cover cyberspace,¹² and ensuring that we continue to innovate and enjoy military superiority in the cyber arena,¹³ as well as his leadership as Ranking Member of both the House Financial Services Committee's Artificial Intelligence and FinTech Task Forces.¹⁴ I absolutely agree with the Ranking Member's view that we must continue to take strong action to deter potential Russian interference in American elections going forward, particularly as we approach the Presidential election in November,¹⁵ that we must build a true transatlantic partnership when it comes defending our allies in cyberspace and that NATO must play a vital

⁶ See, e.g., Robert Walton, *Utilities on High Alert as Phishing Attempts, Cyber Probing Spike Related to Coronavirus*, Utility Dive (Mar. 9, 2020), available online at <<https://www.utilitydive.com/news/utilities-on-high-alert-as-phishing-attempts-cyber-probing-spike-related-t/573698/>>; see also GEN (ret.) Keith B. Alexander & Jamil N. Jaffer, *Iranian Cyberattacks Are Coming, Security Experts Warn*, Barron's (Jan. 10, 2020), available online at <<https://www.barrons.com/articles/u-s-companies-should-brace-for-iranian-cyberattacks-security-experts-warn-51578306469>>.

⁷ See *id.*; GEN (ret.) Keith B. Alexander & Jamil N. Jaffer, *Only a Serious Response Will Reverse Iran's Growing Aggression*, The Hill (Oct. 3, 2019) available online at <<https://thehill.com/opinion/national-security/463758-only-a-serious-response-will-reverse-irans-growing-aggression>>; GEN (ret.) Keith B. Alexander & Jamil N. Jaffer, *Iran's Coming Response: Increased Terrorism and Cyber Attacks?*, The Hill (Oct. 3, 2019), available online at <<https://thehill.com/opinion/national-security/443610-irans-coming-response-increased-terrorism-and-cyber-attacks>>.

⁸ See, e.g., GEN (ret.) Keith B. Alexander & Jamil N. Jaffer, *We Have a Lot of Work to Do as a Nation — And it Starts with Uniting*, The Hill (June 11, 2020), available online at <<https://thehill.com/opinion/white-house/502107-we-have-a-lot-of-work-to-do-as-a-nation-and-it-starts-with-uniting>>; Jamil N. Jaffer, *A House Divided*, National Security Institute (June 5, 2020), available online at <<https://nationalsecurity.gmu.edu/press-releases/a-house-divided/>>.

⁹ See *id.*

¹⁰ See, e.g., Press Release, *Rep. Hill Discusses Future of Identity Protection During Artificial Intelligence Task Force Hearing*, Office of Rep. French Hill (Sept. 12, 2019), available online at <<https://hill.house.gov/news/documentsingle.aspx?DocumentID=6057>>; Press Release, *Increasing Data Security for Arkansans: Hill's Action on Equifax Breach*, Office of Rep. French Hill (Oct. 20, 2017), available online at <<https://hill.house.gov/news/documentsingle.aspx?DocumentID=1126>>.

¹¹ See, e.g., Press Release, *Hill: 'Sanctions Against Russia Send a Powerful Message'*, Office of Rep. French Hill (Mar. 15, 2018), available online at <<https://hill.house.gov/news/documentsingle.aspx?DocumentID=1556>>.

¹² See Press Release, *Rep. Hill Delivers Speech at University of Arkansas's Fulbright College: "America and Her Place in a Post-Berlin Wall World"*, Office of Rep. French Hill (Dec. 3, 2019), available online at <<https://hill.house.gov/news/documentsingle.aspx?DocumentID=6371>>.

¹³ *Id.*

¹⁴ See, e.g., Press Release, *House Financial Services A.I. Task Force Mulls Virtual Hearings*, Office of Rep. French Hill (June 21, 2019), available online at <<https://hill.house.gov/news/documentsingle.aspx?DocumentID=5800>>.

¹⁵ See, e.g., GEN (ret.) Keith B. Alexander & Jamil N. Jaffer, *While the World Battles the Coronavirus, Our Adversaries are Planning their Next Attack*, The Hill (Apr. 7, 2020), available online at <<https://thehill.com/opinion/national-security/491322-while-the-world-battles-the-coronavirus-our-adversaries-are>>.

role in this effort,¹⁶ and that our nation is best secured when we maintain a well-resourced military and intelligence community, particularly in the rapidly developing cyber arena.¹⁷ And I likewise personally support your advocacy for a strong American role in the world and the critical importance of protecting religious freedom and promoting religious tolerance around the globe¹⁸ and share your view that these efforts are critical if we are to continue to stand as a nation set apart, destined for leadership, particularly at a time when there are many in this nation who would have us take a significant step back from the world stage.

II. Financial Sector Vulnerabilities and Threats in the COVID-19 Environment

It goes without saying America's financial services sector—at the heart of our economy and success as a nation—has long faced significant, sustained cyber attacks from a wide range of threat actors. In an April 2019 letter to shareholders, Jamie Dimon, the Chairman and CEO of J.P. Morgan Chase, suggested that “[t]he threat of cyber security may very well be the biggest threat to the U.S. financial system.”¹⁹ For the fourth year in a row, in 2019, IBM assessed that the finance and insurance sector was the number one most attacked sector, with attacks on these institutions accounting for 17 percent of all attacks in the top 10 most attacked industries.²⁰ And the Director of National Intelligence in his worldwide threat assessment in early 2019 noted the massive scale of the threat posed by just one nation-state threat actor—North Korea—to financial institutions globally, noting its “attempts to steal more than \$1.1 billion from financial institutions across the world,” one of which was the “successful cyber heist of an estimated \$81 million from the New York Federal Reserve account of Bangladesh’s central bank.”²¹

And yet, even given the significant threat already facing the financial sector, in mid-April 2020—just two months ago—the U.S. Secret Service and FBI jointly issued a warning that “the COVID-19 pandemic provides criminal opportunities on a scale likely to dwarf anything seen before,” noting specifically that “[t]he speed at which criminals are devising and executing their schemes is truly breathtaking” and that the “sheer variety of frauds already uncovered is itself shocking.”²² According to these federal agencies, the cyber fraud in play as a result of the pandemic includes the “targeting [of] websites and mobile apps designed to track the spread of COVID-19 and using them to implant malware to steal financial and personal data,” threat actors

¹⁶ See GEN (ret.) Keith B. Alexander & Jamil N. Jaffer, *A Transatlantic Alliance is Crucial in an Era of Cyberwarfare*, Financial Times (Sept. 4, 2018), available online at <<https://www.ft.com/content/c01a7f94-af81-11e8-87e0-d84e0d934341>>.

¹⁷ See, e.g., GEN (ret.) Keith B. Alexander & Jamil N. Jaffer, *Ensuring US Dominance in Cyberspace in a World of Significant Peer and Near-Peer Competition*, XIX Geo. J. Int'l Aff. 51, 55-57 (Feb. 2018), available online at <<https://nationalsecurity.gmu.edu/wp-content/uploads/2018/10/GJIA-19-1-FINAL-rev-57-72.pdf>>.

¹⁸ See Press Release, Rep. Hill Speech on “America and Her Place in a Post-Berlin Wall World,” *supra* at n. 11.

¹⁹ See Jamie Dimon, *Letter to Shareholders* at 35, JP Morgan Chase (Apr. 2019), available online at <<https://www.jpmorganchase.com/corporate/investor-relations/document/ceo-letter-to-shareholders-2018.pdf>>.

²⁰ See IBM Security, *X-Force Threat Intelligence Index 2020* at 30 (2020), available online at <<https://www.ibm.com/downloads/cas/DEDOLR3W>>.

²¹ See, e.g., Office of the Director of National Intelligence, *Worldwide Threat Assessment of the U.S. Intelligence Community* at 6, Senate Select Committee on Intelligence (Jan. 29, 2019), available online at <<https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf>>.

²² See Federal Bureau of Investigation, *FBI and Secret Service Working Against COVID-19 Threats* (Apr. 15, 2020), available online at <<https://www.fbi.gov/news/pressrel/press-releases/fbi-and-secret-service-working-against-covid-19-threats>>.

“posing as national and global health authorities...to conduct phishing campaigns...designed to trick recipients...into downloading malicious code” and significant efforts deploy ransomware to take advantage of vulnerable individuals and businesses.²³

According to CarbonBlack, ransomware attacks increased 148% in March 2020 over the baseline from the prior month, with the financial sector being the biggest single sectoral target, with a 38% increase in attacks.²⁴ And according to the Financial Stability Institute (FSI) of the Bank of International Settlements (BIS), an international institution owned by key central banks, the FS-ISAC identified over 1,500 high-risk domains created after Jan. 1, 2020 with both a COVID-19 and financial theme.²⁵ States have both in the U.S. and abroad have fallen victim to COVID-related threats. For example, in the United States, we’ve seen massive unemployment fraud in places like Washington State where the state lost hundreds of millions of dollars.²⁶ And in Germany, the state of North Rhine-Westphalia fell victim to a phishing campaign focused on its economic affairs ministry’s COVID-19 relief program which resulted in over 3,000 fake requests being granted, for a total loss of between \$35 million and \$110 million in fraudulent payments.²⁷

When it comes to individual consumers and business end users, the U.S. Department of Homeland Security’s (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the U.K.’s National Cyber Security Centre (NCSC) in April put out an alert highlighting a number of financially related threats conducted by malicious cyber actors exploiting the COVID-19 pandemic.²⁸ Specifically, CISA and NCSC indicated that SMS and email phishing campaigns, including campaigns designed to deploy malware were actively taking advantage of interest in the coronavirus pandemic, including lures spoofing actual COVID-related senders and materials, many of which were deployed for financial gain.²⁹ Likewise, CISA and NCSC reported increasing efforts by threat actors to take advantage of the new work from home environment, with increasing efforts by threat actors to exploit publicly know vulnerabilities in remote access software including Citrix and Microsoft RDP.³⁰ In the same month, Google reported that it was seeing 18 million daily malware and phishing emails related to COVID-19, not to mentioned more than 240 million COVID-related daily spam messages.³¹

²³ *Id.*

²⁴ See VMware Carbon Black, *Amid COVID-19, Global Orgs See a 148% Spike in Ransomware Attacks; Finance Industry Heavily Targeted* (Apr. 15, 2020), available online at <<https://www.carbonblack.com/2020/04/15/amid-covid-19-global-orgs-see-a-148-spike-in-ransomware-attacks-finance-industry-heavily-targeted/>>.

²⁵ See Juan Carlos Crisanto and Jenny Prenio, *Financial Crime in Times of COVID-19 – AML and Cyber Resilience Measures*, FSI Briefs, No. 7 (May 2020), at 1, available online at <<https://www.bis.org/fsi/fsibriefs7.pdf>>.

²⁶ See Paul Roberts, et al, *‘Hundreds of Millions of Dollars’ Lost in Washington to Unemployment Fraud Amid Coronavirus Joblessness Surge*, Seattle Times (May 21, 2020), available online at <<https://www.seattletimes.com/business/economy/washington-adds-more-than-145000-weekly-jobless-claims-as-coronavirus-crisis-lingers/>>.

²⁷ See Catalin Cimpanu, *German Government Might Have Lost Tens of Millions of Euros in COVID-19 Phishing Attack*, ZDNet (Apr. 18, 2020), available online at <https://www.zdnet.com/article/german-government-might-have-lost-tens-of-millions-of-euros-in-covid-19-phishing-attack/?web_view=true>.

²⁸ See Department of Homeland Security, *COVID-19 Exploited by Malicious Cyber Actors*, CISA Alert AA20-099A (Apr. 8, 2020), available online at <<https://www.us-cert.gov/ncas/alerts/aa20-099a>>.

²⁹ *Id.*

³⁰ *Id.*

³¹ See Steven Musil, *Google Blocking 18M Malicious Coronavirus Emails Every Day*, CNET (Apr. 15, 2020), available online at <<https://www.cnet.com/news/google-seeing-18m-malicious-coronavirus-emails-each-day/>>.

And these larger issues have a direct impact on the financial industry. Specifically, FSI estimates that globally, approximately 300 million workers are working from home, including up to 90% of banking and insurance employees.³² This situation has implications for the financial industry beyond just the potential vulnerability of employees working online. For example, FSI assesses that because banks are increasingly required to identify and onboard new customers wholly or largely online, and because many regulatory and oversight bodies have provided extraordinary relief on standard anti-money laundering requirements, including identification verification and filing requirements, the COVID-19 situation creates significant opportunities for illegal exploitation and operational risk.³³

And all of this is taking place, as a pair of Carnegie Europe experts point out, in the course of a massive effort by the U.S. and other governments around the globe to inject new capital into their national and regional economies, an effort that has at its heart, the very global financial system that is the primary target of well-resourced nation-state and non-nation-state attackers.³⁴ Specifically, given the new pandemic environment, FSI assesses that there is an increased likelihood for the misuse of online financial services for money laundering as well as possible corruption or misuse of government stimulus funds and international financial aid.³⁵ Thus, even though financial institutions have long been under significant pressure in cyberspace, it is the massive scale and nature of the threat—particularly in the COVID-19 environment—that truly creates the tough challenges. Indeed, in mid-April 2020, the U.S. Departments of State, the Treasury, and Homeland Security, and the Federal Bureau of Investigation jointly issued an advisory indicating that North Korea’s “malicious cyber activities threaten the United States and the broader international community and, in particular, pose a significant threat to the integrity and stability of the international financial system.”³⁶

In particular, the U.S. government noted North Korea’s “capability to conduct disruptive or destructive cyber activities affecting U.S. critical infrastructure” as well as its “use[] [of] cyber capabilities to steal from financial institutions,” and specifically highlighted three areas of North Korean financial crime: (1) the use of cyber-enabled financial theft and money laundering, with the amount of these efforts amount almost doubling over the course of 2019, putting North Korea’s total theft attempts at as much as \$2 billion by late 2019; (2) extortion campaigns, where North Korean cyber actors seek ransom payments either on their own behalf or that of third parties by compromising an entity’s network and threatening to shut it down; and (3) cryptojacking, where North Korean actors seek to compromise a victim machine and steal its computing resources to mine digital currency.³⁷

This high-level description of the significant threats facing the U.S. and global financial industry is not meant to be alarmist. Indeed, it is important to note that the industry has taken significant

³² See Crisanto & Prenio, *Financial Crime*, *supra* n. 25 at 2.

³³ *Id.* at 2-4, 6-8.

³⁴ See Tim Maurer & Arthur Nelson, *COVID-19’s Other Virus: Targeting the Financial System*, Carnegie Europe (Apr. 21, 2020), available online at <<https://carnegieeurope.eu/strategieurope/81599>>.

³⁵ *Id.* at 2.

³⁶ See DHS, *Guidance on the North Korean Cyber Threat*, CISA Alert AA20-106A (Apr. 15, 2020), available online at <<https://www.us-cert.gov/ncas/alerts/aa20-106a>>.

³⁷ *Id.*

steps to get ahead of the challenges presented by these capable threat actors. For example, in his April 2019 letter, J.P. Morgan CEO Dimon specifically noted the “enormous effort and resources” dedicated by banks like J.P. Morgan to cyber defense efforts, estimating that his institution alone spends “nearly \$600 million a year on [cybersecurity] and [has] more than 3,000 employees deployed to this mission in some way.”³⁸ And J.P. Morgan is not alone: in 2018, Deloitte and the FS-ISAC conducted a survey that estimated that the average bank spent about \$2,300 per employee on cybersecurity, or about 10% of their overall IT budget.³⁹

Importantly, while IBM’s data on the targeting of the finance and insurance sector indicates that companies in this industry “tend to experience a higher volume of attacks relative to other industries” they are also “likely to have more effective tools and processes in place to detect and contain threats before they turn into major incidents.”⁴⁰ Financial sector companies have also taken significant steps to protect their assets in the event of a breach, including preparing and testing strong individual incident response plans and through the creation of joint resilience efforts like the FSARC. And these efforts appear to have been somewhat effective at mitigating damages from data breaches, with estimates indicating a mitigation rate of approximately 10%.⁴¹

At the same time, it is hard to overstate the potential systemic implications of cyber attacks on the financial sector. In early February 2020, just before the coronavirus became a central focus of everyone’s attention, *The Independent*, a British newspaper reported that Christine Lagarde, the President of the European Central Bank (ECB) had recently warned that there are “several ‘plausible channels’ through which a cyber attack could morph into a serious financial crisis.”⁴² Lagarde was citing a report issued by the European Systemic Risk Board (ESRB) which identified scenarios under which “a cyber incident could, under certain circumstances, rapidly escalate from an operational outage to a liquidity crisis.”⁴³

In assessing these risks, the ESRB noted that cyber risk possesses certain features that make it fundamentally different in nature than most other operational risks.⁴⁴ These features including the speed and scale with which such risks spread across entities, sectors, and borders, the way such risks spread to organizations that aren’t the original targets of the attack, as well as the potential intent of the attackers in the cyber arena, which can go well beyond mere financial gain to attempts to cripple a nation and its economy.⁴⁵ The ESRB therefore looked at situations where there was high potential for a cyber incident to erode trust in the financial system, either because of large potential losses or where there is destruction, encryption or alteration of data

³⁸ *Id.*

³⁹ See Sam Friedman & Nikhil Gokale, *Pursuing Cybersecurity Maturity at Financial Institutions*, Deloitte (May 1, 2019), available online at <<https://www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html>>.

⁴⁰ See IBM X-Force 2020 Report, *supra* n. 20 at 30.

⁴¹ *Id.*

⁴² See Phil Thornton, *Cyber Attacks Could Cause Financial Crisis, Says ECB Chief Christine Lagarde*, *The Independent*, available online at <<https://www.independent.co.uk/news/business/news/cyber-attack-financial-crisis-christine-lagarde-ecb-a9322556.html>>..

⁴³ See European Systemic Risk Board, *Systemic Cyber Risk* (Feb. 2020), at 3, 27-39, available online at <https://www.esrb.europa.eu/pub/pdf/reports/esrb_report200219_systemiccyberrisk-101a09685e.en.pdf>.

⁴⁴ *Id.* at 2.

⁴⁵ *Id.*

related to value, in order to determine whether such situations could turn an operational crisis at one entity into a systemic one where national or global financial liquidity might be at stake.⁴⁶

Specifically, the ESRB looked at three major real-world cyber attacks: (1) the spread of the North Korean-authored WannaCry ransomware in 2017 that infected over 200,000 computers globally in over 150 countries and is estimated to have cost between several hundred million dollars to \$4 billion; (2) the Russian NotPetya attack on Ukraine in 2017 that caused approximately \$10 billion in damage globally, the bulk of which was to private sector companies like Maersk, that had only limited exposure to Ukraine; and (3) the 2018 Cosmos Bank theft—attributed by some to North Korea—of over \$10 million that was withdrawn in 14,000 coordinated transactions across 28 countries within two hours.⁴⁷ The ESRB's goal was to determine why those attacks, while significant, did not result in systemic problems for the global financial system.⁴⁸ In each of those cases, ESRB's analysis indicated that rather than systemic capabilities protecting the global financial system from these attacks, the reality was that we were able to escape major global damage as a result of decisions made by the attackers. For example, with respect to WannaCry, the ESRB assessed that the fortuitous discovery of a kill switch fairly early into its propagation led to a significant limiting of its potential global effect.⁴⁹ With respect to NotPetya, the ESRB assessed that had the tool been more broadly targeted by Russia at global financial institutions rather than at a key piece of Ukrainian software that also happened to be used by a handful of large international companies like Maersk, it could easily have caused major systemic damage.⁵⁰ And with Cosmos Bank, the ESRB assessed that the high level of coordination and penetration suggests the attackers could have done significantly more damage to Cosmos Bank (and potentially others), had they simply chosen to do so and could thereby have caused large spillover effects to other institutions and counterparties.⁵¹

The ESRB also looked at a series of hypothetical scenarios: (1) the incapacitation of the payments systems of a domestic systemically important bank (D-SIB); (2) the malicious destruction of account balance data; and (3) the scrambling of price and position data.⁵² And the ESRB's results were stark and troubling. Even in the D-SIB scenario, which was the least aggressive of three hypothetical scenarios, the ESRB assessed that the unavailability of payments systems and account balances could not only undermine confidence in the affected bank, but also might lead to spillover effects to other sister institutions and counterparties, including small-and-medium sized businesses outside of the financial sector that might rely on the incoming payments to make payroll and other outbound payments.⁵³ When combined with potential fake news about the actual cause of the situation and its impact on the individual bank, the ESRB assessed that such a scenario could lead to large-scale instability, particularly if the counterparty issues spread more broadly, potentially causing a lack of confidence in other financial institutions.⁵⁴ In the malicious destruction scenario, the ESRB assessed that the threat actors

⁴⁶ *Id.* at 2-3, 27-39.

⁴⁷ *Id.* at 27-30.

⁴⁸ *Id.* at 24, 27-30.

⁴⁹ *Id.* at 28.

⁵⁰ *Id.* at 29.

⁵¹ *Id.* at 30.

⁵² *Id.* at 30-36.

⁵³ *Id.* at 30-31.

⁵⁴ *Id.* at 31-32.

would also attack business continuity and technical recovery procedures meaning that some of the data might be permanently lost.⁵⁵ In such a scenario of actual data loss, the ESRB assessed that this might cause a need for emergency funding from the government or other institutions and ultimately might result in the bank being unable to meet its collateral requirements, triggering potential defaults.⁵⁶ The combination of this situation with potential use of social media by the attacker to magnify concerns could also cause a significant loss of consumer confidence again potentially causing systemic effects.⁵⁷ Finally, with respect to the malicious manipulation of price feeds and position information, the ESRB assessed that the damage could be massive, leading to distressed liquidation of assets and severe market turmoil.⁵⁸ Specifically, in the view of the ESRB analysts, as uncertainty about regarding the reliability of prices and positions started to flow into the market causing trades to fail settlement, traders become likely to exit the market, eventually leading to a liquidity crisis, increased volatility, price drops, and margin calls, among other things, with some firms being forced to default and, again, potentially significant systemic effects.⁵⁹

This comprehensive analysis by the ESRB highlights the systemically interconnected nature of the financial services industry and flags how a successful attack—even at a single institution—if large enough and serious enough—could cause systemic issues and potentially undermine financial industry stability at a national and global scale. In order to address these issues, national financial supervision authorities have already begun to take significant action, particularly given the unique nature of potential threats coming out of the current pandemic.

Specifically, in the context of coronavirus, the ECB issued guidance to banks in March 2020 and again in May 2020 noting most recently that “[e]nsuring comprehensive IT and cyber security is [] vital” in particular because banks have “become exceptionally reliant on IT systems owing to the coronavirus (COVID-19) pandemic, which has led to temporary branch closures and the introduction of remote working arrangements on an unprecedented scale.”⁶⁰ In addition, many other international bodies are asking their supervised institutions to remain alert to these heightened risks, and some are going so far as to describe resilience measures that ought be taken.⁶¹

These efforts include additional reviews of potential threats, relying more heavily on information exchange efforts, focus on telework-specific vulnerabilities, examine third party risks, putting in place strong business continuity and incident response plans, and increasing training at subject institutions.⁶² Specifically, the ESRB and BIS’s Cyber Resilience Coordination Center (CRCC) are looking to do more in the information sharing space and according to FSI, the ECRB members have “have agreed to share more cyber information and intelligence, with the aim of

⁵⁵ *Id.* at 32-33.

⁵⁶ *Id.* at 33-34.

⁵⁷ *Id.* at 34.

⁵⁸ *Id.*

⁵⁹ *Id.* at 35-36.

⁶⁰ See European Central Bank, *Guarding Against IT and Cyber Risk* (May 13, 2020), available online at <https://www.bankingsupervision.europa.eu/press/publications/newsletter/2020/html/ssm_nl200513_1_en.html>.

⁶¹ *Id.* at 4.

⁶² *Id.* at 5.

identifying cyber threats and exchanging best practice[s] to prevent attacks.”⁶³ And one of the FSI’s core recommendations to financial authorities and institutions globally is to engage in the “active sharing of information between the public and private sectors, and within and between jurisdictions.”⁶⁴

III. Recommendations

As the Committee continues its efforts to address these critically important matters, it may wish to consider a handful of specific initiatives that could be implemented in the near future and could have a significant beneficial effect on the ability of financial institutions to protect against and respond to significant cyber threats in the current environment.

A. Move Secret Service to the Treasury Department and Provide It with Additional Investigative Authorities and Resources.

At least one key former government official, Juan Zarate, who previously served as the first-ever Assistant Secretary of the Treasury for Terrorist Financing and Financial Crimes in the Bush Administration, and Tim Maurer, the head of the Cyber Policy Initiative at the Carnegie Endowment for International Peace, have recently argued in favor moving the U.S. Secret Service—which has long had a central role protecting the financial sector—back to the Treasury Department from the Department of Homeland Security.⁶⁵ Zarate and Maurer argue that such a move could “better align policy, regulatory, intelligence and enforcement attention on protecting the integrity and resilience of the American financial system.”⁶⁶ The current Administration supports this effort, having proposed such a move in its FY2021 budget submission to Congress.⁶⁷

News reports have suggested that an internal feasibility study conducted by the Secret Service determined that “moving the Secret Service would help enhance collaboration in the Treasury and would put the Secret Service back on the map as a large law enforcement agency, though it could harm morale at [DHS]...[and could] ‘open DHS up to additional reforms or reorganizations, perhaps even some involving the transfer or dismantling of other operating components, further weakening the department at a critical time in its development.’”⁶⁸ While the impact on DHS is important to consider, the Committee should take the action most likely to result in better cybersecurity for the critically important financial sector.

⁶³ *Id.* at 6.

⁶⁴ *Id.* at 8.

⁶⁵ See Juan Zarate & Tim Maurer, *Protecting the Financial System Against the Coming Cyber Storms*, The Hill (May 18, 2020), available online at <<https://thehill.com/opinion/cybersecurity/498244-protecting-the-financial-system-against-the-coming-cyber-storms>>.

⁶⁶ *Id.*

⁶⁷ See Neils Lesniewski, *White House Budget Plan has Secret Service Back under Treasury*, Roll Call (Feb. 10, 2020), available online at <<https://www.rollcall.com/2020/02/10/white-house-budget-plan-has-secret-service-back-under-treasury/>>.

⁶⁸ See Colleen Long, *Secret Service May Leave Homeland Security, Rejoin Treasury*, Associated Press (Feb. 7, 2020), available online at <<https://www.pbs.org/newshour/politics/secret-service-may-leave-homeland-security-rejoin-treasury>>.

Even though there are undoubtedly challenges with such an effort, on balance the benefits of such a move are likely to outweigh the costs. And regardless whether the Committee acts on legislation to move the Secret Service back to the Treasury Department, it is likewise important that the Committee strongly consider provide additional resources to U.S. Secret Service to investigate and directly address the very real cyber threats to financial institutions identified in this testimony and also consider appropriate modifications to U.S. Secret Service's investigative authorities to support its work in this area.

B. Create an Operational Capability at the Treasury Department to Work with Industry to Address Cyber Threats

The Treasury Department has long played a leading role in working directly with key financial institutions to understand and mitigate cyber risk. The Committee ought consider providing Treasury with the opportunity to build on this highly important and effective work through the creation of a Financial Threats Cyber Operation Center (FT-CyOC) that would have access to real-time threat intelligence from the national security community, including DHS, FBI, NSA, and U.S. Cyber Command, as well as directly from the financial services industry with appropriate liability and other protections provided by the Cyber Information Sharing Act of 2015.

Such a capability, if provided by the Committee, would allow Treasury to collaborate directly with the financial sector on active threats and to tip national security organizations to intelligence needs of industry as well as the behaviors of potential threat actors being seen across the industry. Likewise, such a capability would allow Treasury to leverage its position as an intelligence community member, through its Office of Intelligence and Analysis, to collect and share threat intelligence, in real-time, back to industry in an actionable form while still appropriately protecting intelligence sources and methods.

Most importantly, the FT-CyOC ought serve not simply as an information sharing mechanism, but also should work directly with industry and government partners to enable them to take action against such threats as they happen. Placing this capability at Treasury would specifically allow the Department to take advantage of the trusted relationships it has already built with key industry players and organizations, including but not limited to the FS-ISAC and FSARC, as well as its already strong existing relationships with key cyber players in government, including across the national security community.

C. Implement a True Collective Defense Framework for the U.S. Financial Sector and Government and Support the Creation of a Joint Collaborative Environment

The Cyberspace Solarium Commission recently noted that “[t]he U.S. government and industry ... must arrive at a new social contract of shared responsibility to secure the nation in cyberspace.”⁶⁹ According to the Commission, “[t]his ‘collective defense’ in cyberspace requires that the public and private sectors work from a place of truly shared situational awareness and

⁶⁹ See Cyberspace Solarium Commission, *Commission Report* (March 2020), at 96, available online at <<https://www.solarium.gov/report>>.

that each leverages its unique comparative advantages for the common defense.”⁷⁰ Specifically, the Commission noted that “[w]hile the U.S. government has taken a number of steps to develop situational awareness in cyberspace, there continue to be significant limitations on its ability to develop a comprehensive picture of the threat...the data or information is not routinely shared or cross-correlated at the speed and scale necessary for rapid detection and identification.”⁷¹

To that end, the Commission recommended the creation of a joint collaborative environment, “a common, cloud-based environment in which the federal government’s unclassified and classified cyber threat information, malware forensics, and network data from monitoring programs are made commonly available for query and analysis.”⁷²

The Committee should consider supporting this effort and working to provide full funding for the creation and standup of this environment, as well as appropriately resourcing the Treasury Department to play a central role in this environment alongside the financial sector.

D. Launch Efforts with Key Allies to Strengthen International Threat Sharing, Response and Deterrence Capabilities

In terms of international actions, Carnegie Europe is right to recommend that the international community “need a vision and a multi-year strategy to connect the fragmented lines of effort to strengthen cybersecurity in the global financial system” in particular when it comes to “increasing operational resilience [and] deterring malicious actors.”⁷³ That being said, more concrete actions in the near-term are also critical. To that end, as recommended by Messrs. Zarate and Maurer, the United States should take advantage of its year-long G7 presidency to “launch a process similar to its creation of the Financial Action Task Force [FATF] in 1989.” The FATF, which Zarate and Maurer correctly note is “[t]he cornerstone of today’s global anti-money laundering efforts,” developed out of a prior G7 effort.⁷⁴ Like that earlier AML-focused effort, the United States could work with key allies to establish a broader international coalition—grounded in core concepts of cyber collective defense—that would permit nations with sometimes disparate agendas to collaborate with one another and their respective private sectors on cyber defensive measures.⁷⁵ Similarly, such a forum could serve to buttress international efforts to expand and enforce the use of sanctions against cyber threat actors.⁷⁶

In addition, the United States should work closely with allies in Europe, and specifically NATO allies to strengthen its deterrence capability when it comes to common threat actors, like China, Russia, Iran, and North Korea, and actually be prepared to take action pursuant to the recent public assertion by the NATO Secretary General that NATO would exercise its Article V collective defense provisions in response to a major cyberattack.⁷⁷

⁷⁰ *Id.*

⁷¹ *Id.* at 101.

⁷² *Id.* at 102.

⁷³ See Maurer & Nelson, *COVID-19’s Other Virus*, *supra* n. 34.

⁷⁴ See Zarate & Maurer, *Protecting the Financial System*, *supra* n. 65.

⁷⁵ *Id.*

⁷⁶ *Id.*

⁷⁷ See Jens Stoltenberg, *NATO will Defend Itself*, Prospect Cyber Resilience Supplement (Aug. 29, 2019), available online at <https://www.nato.int/cps/en/natohq/news_168435.htm?selectedLocale=en>.

This will require holding our NATO allies to their existing commitments with respect to their defense budgets and working with them to ensure that sufficient resources are being spent across the alliance on cyber defense and offensive capabilities. Such spending is critical to both better protect critical national infrastructures, including financial institutions, as well as hold at risk the systems of potential cyber adversaries to effectively deter significant destructive or disruptive attacks. It will also require NATO allies to engage in a more robust threat sharing to not only share known malware, but also create true shared situational awareness across the core NATO member states in order to allow them to collaborate in real-time to triage and take action against regional threats,⁷⁸ in a manner similar to the joint collaborative environment recommended above for U.S. industry and government by the Cyberspace Solarium Commission.

Conclusion

Thank you again for the opportunity to present my views to the Committee. I look forward to your questions and ideas.

⁷⁸ See Alexander & Jaffer, *Transatlantic Alliance*, *supra* n. 16; see also Jason Miller, *DoD, NATO Turn to Collective Defense against Cyber Attacks*, Federal News Network (June 28, 2019), available online at <<https://federalnewsnetwork.com/ask-the-cio/2019/06/dod-nato-turn-to-collective-defense-against-cyber-attacks/>>.

Written Statement

Tom Kellermann
 Head of Cybersecurity Strategy
 VMware, Inc.
 Before the U.S. House of Representatives, Committee on Financial Services, Subcommittee on National Security, International Development and Monetary Policy

June 16, 2020

Chairman Cleaver, Ranking Member Hill, Members of the Subcommittee, I am Tom Kellermann, Head of Cybersecurity Strategy for VMware Inc. I have over 20 years of experience in cybersecurity. VMware is the fifth largest software company in the world. We have revenues of over \$10 billion and more than 31,000 employees. We are headquartered in Silicon Valley, California, with 125 offices throughout the world, serving more than 75,000 partners and 500,000 customers, including 100 percent of the Fortune 500. Our software is present in 88 percent of the world data centers and was the enabler for data center consolidation worldwide, savings organizations billions in hardware costs. Thank you for the opportunity to testify before the Subcommittee today.

America is grappling with a cyberinsurgency and our financial sector is the number one target. A recent report issued by the World Economic Forum's (WEF) "[Global Risks Report 2020](#)" states that cybercrime will be the second most-concerning risk for global commerce over the next decade and the Darkweb economy of scale will become the third largest economy in the world by 2021. During the first five months of 2020 alone, cyberattacks against the financial sector increased by 238 percent, according to VMware Carbon Black data. Cybercriminals are capitalizing on COVID-19, and they are doing so in tandem with the news cycle.

The financial sector is facing a myriad of highly sophisticated threats. Although the sector is generally more secure than other industry, it is facing the world's elite hackers, composed of organized crime syndicates and motivated nation-states. Geopolitical tension is manifesting in cyberspace.

A few rogue nation state threat actors have been offsetting economic sanctions via attacks on Society for Worldwide Financial Telecommunications (SWIFT) and other payments systems. Hidden Cobra out of North Korea is one group that embodies this phenomenon. VMware's Carbon Black has conducted several in depth analysis over the years, detailing the trends and threats facing the industry. I have sent to the Subcommittee our latest report which highlights how financially motivated criminals have escalated bank heists to cyber-hostage situations. Over the past six months, cyber defenders have seen a high level of coordination from cybercriminals, who are demonstrating significant innovation to maintain persistence and counter incident response efforts.

At an alarming rate, transnational organized crime groups are leveraging specialist providers of cybercrime tools and services to conduct a wide range of crimes against financial institutions, including ransomware campaigns, business email compromise (BEC) scams and access mining. Criminals are increasingly sharing resources and information and reinvesting their illicit profits into the development of new, even more destructive capabilities. The growing availability of ready-made malware is creating opportunities for even inexperienced criminal actors to launch their own operations. When combined with a steady commercial growth of mobile devices, cloud-based data storage and services, and digital payment systems, cybercriminals today have an ever-expanding host of attack vectors to exploit. Every

organization—providers of financial services, in particular—must remain vigilant in the face of these evolving threats.

According to the Modern Bank Heists Report which we just released, 80 percent of surveyed banks said they've seen an increase in cyberattacks over the past 12 months, marking a 13 percent increase over 2019. The Bank Heist has now escalated to a hostage situation. 2020 has offered a glimpse into a brave new world. The cybercriminal community has educated themselves as to the interdependencies that exist in the financial sector and they have begun to commandeer these very interdependencies to manifest criminal conspiracies. Thirty three percent of surveyed financial institutions said they've encountered island hopping, an attack where supply chains and partners are commandeered to target the primary financial institution (FI) and subsequently the digital infrastructure of the FI is hijacked and used to attack their customers. 25% of surveyed financial institutions said they were targeted by destructive attacks over the past year. Destructive attacks are rarely conducted for financial gain. Rather, these attacks are launched to be punitive by destroying data. The financial sector is not alone, as the recent FISMA Annual Report to Congress (Fiscal Year 2019) stated that "Attrition" e.g. integrity attacks against federal agencies had significantly increased.

Cybercriminals are evolving in both attack sophistication and organization. We must pay close attention to how we respond to these threat actors and what their ultimate goal is—hijacking digital transformation efforts via island hopping. Trust and confidence in the safety and soundness in the US financial sector is dependent on cybersecurity.

The international financial system is constantly facing new threats as technology proliferates and diversifies. Increasingly, individuals and syndicates use these systems to bypass traditional indicator and warning systems relied upon by regulators and law enforcement. According to a recent FBI statistic, "three in four money laundering cases involve digital currencies." While digital currency is still a relatively specialized market, there are increasing number of security breaches and thefts on digital currency exchange platforms as well as misuse of these platforms by cybercriminals to launder stolen monies. This is because there are few cryptocurrency exchanges that perform Know Your Customer (KYC) procedures and basic security checks, both of which have been commonplace protocols in major exchanges for over a decade. Money laundering can easily take place in these virtual environments, as they can provide high levels of anonymity and low levels of detection.

Money laundering through digital currency and payment systems is just one example of illicit activity online. Other criminal markets include child pornography, weapons and drug sales, hackers and murder for hire, zero-day exploits, and false identity documents. The advent of these criminal markets enabled by anonymous virtual currencies have created a global bazaar for criminals and organized crime to reach a mass global market. Collectively, these digital infrastructures represent a "3-legged stool" of illicit activity: it allows for the storage of illicit goods and services, it provides utility of financial vehicles to allow for the exchange of goods and services, and it develops techniques to successfully transport the illicit goods and services around the world.

In addition to organized crime, extremist organizations are also known to use cryptocurrency and alternative payment systems for operational purposes and to raise funds. Many of these payment services and cryptocurrencies offer true or relative anonymity. For many users, privacy rather than anonymity may be their primary interest, as they do not seek to hide illegitimate behavior. However, the anonymity offered by some of these systems facilitate illicit financial flows (IFF) as well as offering privacy. Advice is available on various social media platforms regarding jihadists' potential use of Dark Wallet, a bitcoin wallet that provides anonymity, and on how to set up an anonymous donation system to send money using bitcoin. This advice is clearly motivated to mask the provision of funds to ISIL. This raises the necessity of increased regulation of digital money.

Cyberspace is not a peaceful environment. In 2020 cybercrime conspiracies will become increasingly punitive and destructive. As the use of virtual currencies and financial systems continues to increase and innovate, so too does global crime. Fintech firms themselves present significant 'operational risks,' lacking the incentive for proper intrusion detection or Know Your Customer (KYC) Anti Money Laundering (AML) protocols under the Bank Secrecy Act. Given that 50 percent of all crimes now have a cyber component, it is high time that we follow the money to create an international e-forfeiture fund.

The modern epidemic of cybercrime and cyberespionage can also be mitigated through modernization of existing authorities to empower the Financial Action Task Force (FATF), the Financial Crimes Enforcement Network (FinCEN) and the Treasury Forfeiture Fund (TFF) to combat cyber-money laundering. Virtual currencies and other alternative payment systems that facilitate money-laundering associated with cybercrime, as well as terrorist financing, must be held to account.

Every digital payment service should abide by KYC and cooperate in all law enforcement initiatives regarding cybercrime conspiracy, or it should be shut down. We can prioritize this effort through the establishment of an international Fund, maintained by the forfeiture of all money laundering and terrorist financing seizures. Proceeds from the Fund will be allocated specifically to critical infrastructure protection of the global financial system. The Fund would represent a global public/private partnership to combat money laundering using these alternative payment systems.

Furthermore, creating global, enforceable rule sets through such a public/ private partnership could help the private sector flourish and simultaneously meet the needs of the unbanked and underbanked throughout the world. Virtual currencies who refuse to know their customers or freeze accounts of those engaged in criminal conspiracies should be subject to Treasury Executive Office for Asset Forfeiture (TEOAF).

In closing, I would like to highlight six opportunities for legislative action for the Subcommittee's consideration:

1. Anti-money laundering and forfeiture regulations must be modernized to seize the virtual currencies and digital payments which are used in the cybercrime conspiracies. These seized funds should be explicitly allocated to cybersecurity investment across US critical infrastructures. Once cybercriminals turn these seized funds into virtual currencies, it is impossible to track. These monies can't be returned to the victims of these crimes so they could be used to strengthen our cyber protections.
2. Urge the Senate to pass the COUNTER Act (HR 2514) that passed out of the House under Chairman Cleaver's leadership. This important piece of legislation would empower the U.S. Treasury Department to protect our national security and safeguard our financial systems by codifying an information-sharing program between law enforcement, financial institutions, and the Treasury Department, enabling the detection and capture of illegal activity. It would also create new innovation labs to facilitate greater communication and coordination among law enforcement agencies, financial institutions, vendors and technology companies with respect to innovation and new technologies used to comply with the requirements of the Bank Secrecy Act.
3. Charge the Financial Stability Oversight Council (FSOC) chaired by the Department of Treasury with the responsibility to create a framework for regulating cryptocurrencies and developing guidelines for strong protections against money laundering and cybersecurity threats to those marketplaces. Additionally, the FSOC should bring greater cross border clarity to information

sharing requirements and enterprise level cyber protections for the financial services sector by engaging with its overseas counterparts. The resulting framework should be incorporated into the FFIEC Information Security Handbook and include mandating best cyber practices such as regular cyber-threat hunting for shared services providers.

4. Chief Information Security Officers (CISOs) should be elevated to directly report to the CEO of financial institutions. Since the position of the CISO was created, most report to the Chief Information Officers within corporations. However, the CISO – CIO reporting structure represents a potential governance crisis. The defensive mindset of the CISO often conflicts with the uptime, availability, and content-driven goals of CIOs. Another concern relating to this structure is that cybersecurity measures may come second to revenue-generating activities.
5. Establish a tax credit for financial sector companies that dedicate at least 10 percent of their IT budgets towards cybersecurity and could be administered by the IRS. These companies should also be incentivized to comply with the NIST Cyber Security Framework which could be validated by a third party.
6. Support the House passage of S. 3636, the U.S. Secret Service Mission Improvement and Realignment Act of 2020. This bill was introduced by Sens. Lindsey Graham (R-S.C.) and Dianne Feinstein (D-Calif.), the chairman and ranking member of the Judiciary Committee, and moves the Secret Service back to its original home at the Department of Treasury. The Secret Service is best known primarily for protection; however, it also performs financial, counterfeit currency, and cybercrime investigations. The proposed realignment allows the Secret Service to reprioritize its investigative mission and was included in the President's 2021 budget submission.

Chairman Cleaver, Ranking Member Hill, thank you for the opportunity to participate in this important hearing. I am happy to answer any questions the Subcommittee might have.

Written Testimony of Amanda Senn

Alabama Securities Commission Chief Deputy Director and NASAA
Cybersecurity Committee Chair

On behalf of

The North American Securities Administrators Association



June 16, 2020

United State House of Representatives

Committee on Financial Services

Subcommittee on National Security, International Development and Monetary
Policy

“Cybercriminals and Fraudsters: How Bad Actors Are Exploiting the Financial
System During the COVID-19 Pandemic”

I. Introduction

Good Morning, Chairman Cleaver, Ranking Member Hill, and members of the Subcommittee. My name is Amanda Senn, and I am the Chief Deputy Director of the Alabama Securities Commission and Chair of the Cybersecurity Committee for the North American Securities Administrators Association ("NASAA").¹ I am honored to testify before the Subcommittee today on behalf of NASAA about how cybercriminals and fraudsters are exploiting the financial system amid the COVID-19 pandemic.

In the United States, state securities regulators have protected Main Street investors for more than 100 years, longer than any other securities regulator. As the regulators closest to your constituents, with an office in every state, we are on the frontline of investor protection. My colleagues and I are responsible for enforcing state securities laws, including investigating complaints, examining broker-dealers and investment advisers, registering certain securities offerings, and providing investor education programs to your constituents.

States are leaders in civil and administrative enforcement actions, as well as criminal prosecutions of securities violators. Our most recently compiled enforcement statistics reflect that in 2018 alone, state securities regulators conducted 5,320 investigations, leading to more than 2,000 enforcement actions, including 218 criminal actions. In 2018, NASAA members reported enforcement actions involving 758 senior victims. Older Americans are a major target of fraudsters and are particularly vulnerable during this crisis due to the nature of the COVID-19 pandemic.

States also continue to serve a vital gatekeeper function for our capital markets by screening out bad actors before they have a chance to conduct business with unsuspecting investors. In 2018, a total of 4,551 securities license applications were withdrawn because of state action, and an additional 1,032 licenses were either denied, revoked, suspended, or conditioned.

Our focus is on protecting retail investors and history has shown us that opportunistic fraudsters will use COVID-19, as much as they have used other crises, to fleece mom and pop investors. Moreover, state securities regulators have a long history of not only working together with one another but also working alongside our federal counterparts and industry self-regulatory organizations to stop frauds and educate investors.

As I will detail in my testimony, acting within the framework of NASAA, state securities regulators are undertaking decisive action aimed at anticipating and shutting down frauds related to the COVID-19 pandemic and the resulting economic uncertainty. Specifically, NASAA has formed a COVID-19 Enforcement Task Force ("Task Force"), consisting of state and provincial securities regulators, to identify and stop potential threats to investors that arise from the COVID-19 crisis. This initiative is being led by NASAA's Enforcement Section Committee and includes more than 100 investigators from the vast majority of member jurisdictions. The Task Force is using online investigative techniques to identify websites and social media posts that may be offering or promoting fraudulent offerings, investment frauds, and unregistered regulated activities.

II. State Securities Regulators and the Protection of Retail Investors from Fraud

State securities regulators routinely take aggressive actions against a wide variety of actors. From fraudsters engaged in Ponzi or pyramid schemes to companies who mislead investors our

¹ The oldest international organization devoted to investor protection, NASAA was organized in 1919. Its membership consists of the securities administrators in the 50 states, the District of Columbia, Canada, Mexico, Puerto Rico and the U.S. Virgin Islands. NASAA is the voice of securities agencies responsible for grass-roots investor protection and efficient capital formation.

message is simple – if you rip off or defraud investors, we will act. Whether acting independently or collaboratively, such as through the NASAA enforcement framework or in conjunction with our federal regulatory partners, state securities agencies have a long history of pursuing enforcement actions that affect not only the residents of our individual states, but also the citizens of our nation as a whole. Moreover, state securities regulators are uniquely well positioned to protect investors by undertaking proactive measures, in addition to reactive measures, to police the securities markets.

Enforcement and Investor Protection

State securities agencies are usually more nimble than our federal counterparts. Upon identifying a problem, we can move quickly to halt ongoing investment frauds using a range of civil and administrative remedies. The cases we bring can involve localized conduct to practices that harm investors across the country. Notable examples of some of the enforcement actions where the states have led the way to address violative conduct involving a large number of investors and large losses include: the securities fraud investigation of Prudential Bache Securities in the 1980s; the 2003 investigation of sell-side research analysts' conflicts of interest; abusive market timing practices by mutual fund investment advisers, which gave an unfair and illegal advantage to hedge funds and other large entities at the expense of retail investors; and the post-2008 financial crises cases involving subprime mortgage-backed securities and auction rate securities, which resulted in billions of dollars being returned to investors as a result of wrongful conduct.²

As pointed out in the preceding examples, states have been and will continue to be active in a broad range of cases, especially those involving investors in our communities. Indeed, while our mission aligns with that of our federal counterparts, the primary focus of state securities enforcement is on the needs of *retail* investors. State securities regulators are well-suited for this mission because of our geographical and societal nexus to the individuals we serve. Moreover, state securities regulators are able to cultivate relationships and partnerships with local criminal authorities and are often able to achieve justice through criminal channels in cases that U.S. Attorneys may be unable to bring due to limitations on resources and directives governing the allocation of those resources.³ State securities regulators are highly skilled and adept at investigating and prosecuting misconduct. They capably represent the public they serve, and no complaint is too small.

Moreover, in Alabama our office has criminal authority and can work criminal cases from start to finish to ensure fraudsters are swiftly and appropriately punished. Financial crimes can be devastating and having the authority to seek justice on behalf of victims is an honor and a privilege that I have never taken for granted. Too often, smaller cases are overlooked, passed over, or fall through the cracks. But in our local offices, we are better able to serve your constituents because they are our friends and our neighbors. And what may be considered a small loss to some is a devastating loss to the person suffering it. Thus, it is oftentimes in these cases that the state securities regulator discovers true meaning in his or her work, for the victim has nowhere else to turn.

Protecting Investors in the Digital Age

² In Alabama alone, the repurchase of auction rate securities resulting from this action totaled \$1.3 billion, saving Alabamians from defaulting on home loans, ruining their credit, and allowing them to pay their bills.

³ Likewise, FINRA is a national self-regulatory organization where decisions are not necessarily made at the grass roots level but through a hierarchy where the focus is often on systematic issues rather than individual violations. Moreover, FINRA's jurisdiction does not extend to unlicensed individuals. While state securities regulators often partner with the SEC and FINRA, and achieve great results, many cases are outside the jurisdiction of or do not meet the threshold criteria for evaluation from either organization.

The proliferation of technology has changed much about the ways in which we are solicited for investments, manage those investments, and communicate with the companies and individuals who handle those investments. Unfortunately, fraudsters are evolving with technology, and the methods by which they prey on investors are rapidly increasing. The digital world presents numerous and complex obstacles to investigations and prosecutions – from the growing number of actors and schemes, to challenges in identifying online perpetrators and collecting evidence in a forensically sound manner. These challenges pose significant hurdles for regulators who must adapt quickly to the ever-changing landscape of online fraud.

For example, in early June my office received three separate reports pursuant to Alabama's Protection of Vulnerable Adults from Financial Exploitation law, a NASAA model law enacted in Alabama in 2016, which indicated individuals were victims of an online financial fraud scheme. According to the three reports detailing the scheme, the victims had visited the webpage of a reputable online broker to review or access their accounts and discovered that they were unable to login. Upon their attempts, they received a screen with a "help" button. The individuals each reported that they clicked on the button and were instructed to call a "1-800" number. The victims called the number and the individual who answered the phone told the victims that the broker's website was down because "5G towers were being placed in California." That person then instructed the caller to log into his account with information that was provided by the suspect. The victims logged in as instructed and shortly after the victims reported that wire transfers were initiated from their accounts to various banking institutions, some overseas. During an interview with the firm last Friday, our case agent learned that attempted wires from the brokerage accounts held by the firm exceeding \$2.6 million had been initiated by the fraudsters and that \$1.2 million had already been stolen. At this time, it is believed that malware was responsible for redirecting the victims from the legitimate webpage of the broker-dealer to a fraudulent knock-off site. To date, 84 victims nationwide have been impacted, but the numbers are rising. Our interview confirmed that the majority of these victims were ages 60 or older.

At one time, this crime would have been likely perpetrated by a person that local authorities could readily identify, such as a person that the victim may have trusted and/or known in the community. Records could have been obtained memorializing any agreement between the two regarding the investment, subpoenas and/or search warrants could have been issued to gather documents that were not readily available, and the identity of the suspect most likely would have been known or could have easily been discovered. In other words, physical evidence of the crime, sufficient to prosecute, could have been collected with relative ease. In the digital age, prosecutors are confronted with numerous evidentiary challenges which, given limited resources, make it exceedingly difficult to investigate, much less, prosecute, these cases. Cyber criminals have an obvious advantage in that they can remain concealed and anonymous.

NASAA members recognize the constraints on investigating and prosecuting cybercrimes and, moreover, the reality that victims may never recover their losses. Thus, states are dedicating resources to more proactive measures. Here, the goal is to stop the fraudsters from victimizing our residents by identifying emerging risks to deter, reduce, and fight them before they become problems.

The COVID-19 Pandemic has Baited the Hook for Fraudsters

Predicting the latest fraud is sometimes simple; just look at the issues of the day. Fraudsters trade on natural disasters, economic crises, and tragedies to push their schemes. They exploit systemic issues at times when investors are most susceptible to fears such as outliving their money or missing out on the next big investment opportunity. This pattern is familiar to regulators as we have seen plenty

of examples such as the waves of fraud during the dot.com bubble of the 1990s, the post-2008 financial crisis, and the creation and evolution of cryptocurrencies. Today, of course, we have COVID-19.

The pandemic coupled with dramatic volatility in the markets has brought loneliness due to social isolation and concerns for financial security. This is likely the reason that my colleagues and I have seen a significant uptick in the number of financial exploitation cases over the past two months.

To date, dozens of reports of fraud related to the Pandemic have come across my desk. From investments purporting to develop vaccines and other pharmaceutical treatments, to investments with a charitable component falsely claiming to help those affected by COVID-19, these frauds are myriad and run the gamut.

Elderly Investors May be Especially Vulnerable Targets

Sadly, and especially during the COVID-19 pandemic, many seniors are spending time in isolation to protect themselves from infection. Friends and family who may have visited regularly are unable to spend time with them. Many seniors have turned to the Internet as a social outlet and have become heavily reliant on online services for shopping, banking, and the initiation of electronic payments that may have otherwise been paid in person. With many seniors in isolation, friends and family are unable to physically check in and are not able to notice the sometimes small but important changes in behavior that could indicate a person is susceptible to fraud or worse, is being victimized.

In January 2016, NASAA created and approved the Model Act to Protect Vulnerable Adults from Financial Exploitation, or “Model Act,” which provides for reporting of suspected financial exploitation to regulatory agencies and allows firms and advisers to enlist the assistance of state securities regulators to review potential red flags of fraud.⁴ In this area, in particular, state securities regulators have partnered with the industry to help protect seniors from being financially exploited. The Model Act has been enacted in 27 jurisdictions, with more considering legislation. As a result of this law, states have seen increased reports of financial exploitation, many of which might not have otherwise been brought to light. In the past several months, I can report that in Alabama these cases have tripled and most of the reports allege that a cybercriminal is the suspect.

NASAA’s COVID-19 Enforcement Task Force

On April 28, 2020, NASAA announced the formation of the COVID-19 Enforcement Task Force (“Task Force”), consisting of state and provincial securities regulators, to identify and stop potential threats to investors stemming from the COVID-19 pandemic.⁵ Modeled after NASAA’s successful Operation Cryptosweep,⁶ the new initiative is being led by NASAA’s Enforcement Section Committee.

The objective of the Task Force is to disrupt, discourage and deter fraudulent or illegal activities which pose threats to investors before significant losses occur. With these goals in mind, the NASAA membership quickly organized and coordinated this large-scale effort. Instructional webcasts

⁴ Additional information about the NASAA Model Act, including legislative commentary for the 2020 State legislative session, is accessible at: <http://serveourseniors.org/wp-content/uploads/2020/01/NASAA-Model-Act-Updated-Commentary-for-2020-Session-012820.pdf>.

⁵ See: <https://www.nasaa.org/54844/nasaa-forms-covid-19-enforcement-task-force/?qoid=current-headlines>.

⁶ In April 2018, NASAA organized a task force of its member state and provincial securities regulators to begin a coordinated series of investigations into ICOs and cryptocurrency-related investment products. As part of its work, the task force identified many cryptocurrency-related products and hundreds of ICOs in the final stages of preparation before being launched to the public. These pending ICOs were advertised and listed on ICO aggregation sites to attract investor interest. The work of the task force yielded hundreds of investigations and scores of enforcement actions. Additional information about Operation Crypto sweep is accessible at: <https://www.nasaa.org/policy/enforcement/operation-cryptosweep/>.

and tutorials on the details of the operation and logistics were provided to participating jurisdictions. Members share resources and assign tasks according to areas of expertise. The Task Force is presently using online investigative techniques to identify websites and social media posts that may be offering or promoting fraudulent offerings, investment frauds, and unregistered regulated activities.

Importantly, the emphasis of the Task Force is on *proactively* protecting investors against fraud through the broad dissemination of enforcement orders, notices, and warnings. By preemptively identifying and uncovering fraudulent conduct that could result in investor losses, the Task Force can expose or discredit the perpetrator to prevent the public from becoming a victim of fraud. In cases where it is discovered that victims have already fallen prey to the fraud, enforcement actions have and will continue to be instituted, and through coordination with internet service providers and/or social media platforms, websites, posts, threads, and advertisements are being dismantled or removed. In other words, not only are we “poisoning the well,” we are also able to shutter it and prevent the broad solicitation of their fraudulent offerings. During the project, as fraudulent activity and conduct is identified, NASAA members throughout the United States, Canada, and Mexico are engaged in media campaigns to promote public awareness of the schemes and investor education.

Currently, 111 participants from 44 NASAA jurisdictions in the United States, Canada and Mexico are leveraging their experience and using their unique tools to stop schemes and enjoin promoters. At the time of formation, the Task Force had identified over 200,000 coronavirus-related domains, either active or reserved. The matters are classified as either investment-related or non-investment related.

To date, 91 investment-related matters have been identified as potentially fraudulent, and there are 54 active and open investigations. Over a dozen of these investigations have resulted in an administrative action, and 26 financially-related referrals have been made to either third parties, law-enforcement, or other regulatory agencies. In addition, the Task Force has identified 39 other “non-investment related” matters and has made at least 12 referrals, with additional referrals forthcoming.

Schemes Identified by NASAA’s COVID-19 Enforcement Task Force

While the schemes observed by the Task Force are manifold, many involve a cryptocurrency or promote investments that are outside the stock market – perhaps due to recent market volatility. In cases involving digital assets, we generally see promoters holding themselves out as cryptocurrency traders and offering investments in schemes promising lucrative profits. Some are more sophisticated than others. In some cases, there is a charitable component related to coronavirus efforts. Other investment opportunities include oil and gas ventures, real estate, penny stocks, precious metals, and investments in the foreign exchange markets. Based on the solicitations and placements of offers, suspects appear to be targeting seniors and persons with portfolios that are losing or have lost value due to current economic conditions.

For example, Alabama and Texas have enforcement actions against an outfit operating under the name “Ultra Mining LLC” that offered investments related to cryptocurrency mining operations.⁷ To induce investors to purchase the “mining plans,” the company claimed that it donated \$100,000 to UNICEF to fight the coronavirus. Other examples of recent enforcement targets include:

- A promoter using social media and online advertisements to recruit victims into an illegal cryptocurrency scheme by fraudulently claiming he can make lucrative profits by trading cryptocurrency.⁸

⁷ Alabama CD No. 2020-0007 and Texas ENF-20-CDO-1801

⁸ Texas ENF 20-CDO-1804

- A self-described oilman who broadly targets victims through online advertisements and social media, fraudulently claiming he has “developed a process for making money drilling oil even after the crash of the oil markets.”⁹
- A company allegedly based in Los Angeles, California, SwiftTradings, advertised on Instagram and communicated with investors about investment opportunities. The company concocted account statements, promised significant returns, and failed to disclose its preposterous fee schedule, which the company claimed were being assessed due to the COVID-19 pandemic.¹⁰
- An investment advertised through Craigslist that encouraged investors to invest their COVID-19 stimulus checks in his scheme. The ads targeted at least 49 states and 2 countries.¹¹
- A promoter who targets retirees and investors who need supplemental income “due to crash in the economy,” touting his ability to capitalize on volatility in the markets to make lucrative guaranteed returns.¹²
- An advertisement posted on Craigslist that encourages prospective clients to “exploit the current coronavirus crises by trading penny stocks from the pharmaceutical and biotechnology industry whose stocks are experiencing significant price fluctuations due to the pandemic.”¹³

This is merely a snapshot of the investment-related cases that are being reviewed by the Task Force. In addition to investment-related schemes, the Task Force is seeing countless other online frauds, which are being referred to the National Center for Disaster Fraud.¹⁴ For example:

- *Stimulus check fraud.* The Task Force has identified advertisements and notices that appear official and claim that “in order to expediate stimulus checks” individuals should fill out their census form. A link is provided to what appears to be an official census form, which solicits the personal information contained on a census form and gives the fraudsters all of the Personal Identifying Information that they need to steal the victim’s identity.
- *Business identity fraud.* The Task Force has seen the names of legitimate non-profits are being used to solicit donations for coronavirus related medical studies.
- *Theft of personal information.* The Task Force recently discovered a company dedicated to “remembering those who lost their lives in the 1st pandemic of the third millennium of the Gregorian Calendar,” whose website creates the appearance that it is a memorial for deceased persons. Users are asked to enter personal information to access the directory.

⁹ Texas ENF 20-CDO-1802

¹⁰ Alabama CD No. 2020-0010

¹¹ Alabama CD No. 2020-0008; Washington State S-20-2879-20-FC01

¹² Texas ENF-20-CDO-1800

¹³ Alabama CD No. 2020-0009

¹⁴ The National Center for Disaster Fraud is a national coordinating agency within the Department of Justice’s Criminal Division dedicated to improving the detection, prevention, investigation, and prosecution of criminal conduct related to natural and man-made disasters and emergencies, including the COVID-19 pandemic.

- *Personal protective equipment fraud.* The Task Force has found numerous companies fraudulently claiming to sell personal protective equipment, sanitizers, and other products.

The list goes on, as does the work of the Task Force. We believe the Task Force's efforts have prevented and will continue to prevent many from being victimized and from becoming another restitution statistic in our respective agencies. In my experience, these enforcement efforts are effective deterrents to fraud, and the long reach of the Task Force's collective jurisdictions enable it to accomplish it on a large scale.

III. NASAA's Activities and Perspective Relating to Cybersecurity

The egregious character of financial crime is enhanced by technology and our growing dependence on online services. As a result, cyber criminals are on the rise and the financial sector remains a top target. Retail investors and small firms feel the impact, and thus cybersecurity is an area where NASAA proactively acts to protect registrants and investors. Indeed, NASAA members serve not only as regulators but also as resource to small firms in their respective jurisdictions.

NASAA Cybersecurity Initiatives and Partnerships

NASAA's Cybersecurity Committee coordinates and facilitates information sharing between NASAA members, industry participants, and state registrants to evaluate how NASAA can best address cybersecurity. The Committee also organizes and holds a cybersecurity roundtable each year in which experts discuss relevant and trending topics in cybersecurity. The roundtable is available for live streaming to the public, including to state-registered investment advisers.

In addition, NASAA's Investment Adviser Cybersecurity and Technology Project Group develops resources for registrants to assist them in protecting their firms and the personally identifiable information ("PII") they maintain on behalf of their clients. These resources include NASAA's Cybersecurity Checklist for Investment Advisers provided in 2018 and a resource guide for cybersecurity practices. These tools are available free of charge to firms and can be used to help state-registered investment advisers identify, protect, and detect cybersecurity vulnerabilities and to respond to and recover from cyber events. Earlier this year, NASAA updated the checklist and issued detailed guidance on steps state-registered investment advisers could take to better protect client information. To further protect investor PII, and in response to consistently identified cybersecurity deficiencies, on May 21, 2019, NASAA members adopted the Investment Adviser Information Security Model Rule Package.¹⁵

Cybersecurity Examinations of State-Registered Investment Advisers

Cybersecurity is a priority for state securities examiners. Smaller companies are the low hanging fruit for cybercriminals, and when you consider that more than three-fourths of the nearly 18,000 state-registered investment advisers are 1-to 2-person shops it is clear how important cybersecurity should be for these small businesses as well.

In their examinations of state-registered investment advisers in 41 U.S. jurisdictions between January and June 2019, state examiners found deficiencies relating to cybersecurity in more than one-quarter (26%) of their examinations, up from 23% during the last series of coordinated examinations in 2017. The top five cybersecurity-related deficiencies included: no testing of cybersecurity vulnerabilities; a

¹⁵ See: <https://www.nasaa.org/48065/nasaa-members-adopt-investment-adviser-information-security-model-rule-package/>

lack of procedures regarding securing or limiting access to devices; a lack of procedures related to internet connectivity; weak or infrequently changed passwords; and inadequate cybersecurity insurance.¹⁶ As noted above, these findings have spurred NASAA members to continue to focus on the importance of enhanced cybersecurity resources for state-registered advisers.

Cybersecurity Collaboration with Federal Authorities

Finally, NASAA members work closely with the federal government and other federal law enforcement agencies regarding cybersecurity. For example, since 2001, NASAA has served as a member of the Financial and Banking Information Infrastructure Committee (FBIIC).¹⁷ Since state securities regulators are the primary regulators for state-registered investment advisers and co-regulators with the SEC for the broker-dealer community, NASAA's engagement with the FBIIC allows for facilitation of the sharing of information regarding emergency planning and preparedness.

Through monthly meetings and, when needed, daily reports and phone calls, staff from FBIIC member organizations work on operational and tactical issues related to critical infrastructure matters, including cybersecurity within the financial services industry and ultimately the effect on retail investors in the marketplace. From cyber safety and education, protecting networks from ransomware, and security of payment networks, to alerts on "hacktivist" threats, conducting tabletop exercises and disaster and recovery tracking and alerts, NASAA provides a central information source for its state members and provides input to the FBIIC on ground level events.

The senior leaders of FBIIC are the principals from each member organization who meet to provide strategic, policy-level direction to the work being done by FBIIC. Topics range from removing information-sharing impediments and enhancing incident-response planning, to examining financial firms to identify best practices around cybersecurity controls. Our office in Alabama is honored to be the NASAA representative to the FBIIC and the designated member to the FBIIC Principals Group.

IV. NASAA's Perspective on Proffered Legislative Proposals

The Committee has invited NASAA to share its views regarding several legislative proposals that have been posted in connection with today's hearing. Accordingly, I am pleased to express strong support for draft legislation entitled, "Senior Investor Pandemic and Fraud Protection Act" (also known as the "Empowering States to Protect Seniors from Bad Actors Act"), and draft legislation entitled "COVID-19 Restitution Assistance Fund for Victims of Securities Violations Act." I will address them in turn.

1. The Senior Investor Pandemic and Fraud Protection Act

The Senior Investor Pandemic and Fraud Protection Act would implement the Senior Investor Protection Grant Program, originally established and authorized by Section 989(A) of the

¹⁶ See: <https://www.nasaa.org/52507/state-investment-adviser-examinations-find-rising-cybersecurity-deficiencies/>.

¹⁷ Chartered under the President's Working Group on Financial Markets, the Financial and Banking Information Infrastructure Committee (FBIIC) is charged with improving coordination and communication among financial regulators, promoting public-private partnerships within the financial sector, and enhancing the resiliency of the financial sector overall. Additional information about the FBIIC is accessible at <https://www.fbiic.gov>.

Dodd-Frank Act, but never put into effect.¹⁸ The bill would also expand the scope of the grants to explicitly include fraud related to COVID-19. Under the bill, qualifying states and state regulators would be able to apply for up to \$500,000 annually in grant funding to combat financial fraud of seniors and vulnerable adults, including cases related to the pandemic, for a maximum of two consecutive years, for a total of \$1 million.¹⁹ The grant funds could be used for such purposes as: hiring staff to investigate cases involving fraudulent marketing related to the pandemic; funding technology, equipment, and training for prosecutors to increase the prosecution of salespersons who target seniors and vulnerable adults; and providing educational materials to seniors and vulnerable adults to raise awareness of misleading or fraudulent marketing.

NASAA strongly supports the Senior Investor Pandemic and Fraud Protection Act.²⁰ Indeed, such legislation is one of state securities regulators' highest priorities for the 116th Congress.²¹

Evidence suggests that as many as one out of every five citizens over the age of 65 has been victimized by financial fraud.²² According to research published by the Consumer Financial Protection Bureau ("CFPB"), financial institutions have reported over 180,000 suspicious activities targeting older Americans since 2013. While the total financial loss is hard to determine, the estimated losses of older adults due to exploitation ranges from \$2.9 billion to \$36.5 billion annually.

Moreover, Congress has repeatedly recognized that seniors are especially susceptible to fraud and agreed on a bipartisan basis regarding the importance of supplementing state resources to educate and protect senior investors. Amid the COVID-19 pandemic, Congress should assist state regulators in securing resources to combat financial exploitation against those most vulnerable in this crisis.²³

2. The COVID-19 Restitution Assistance Fund for Victims of Securities Violations Act

The COVID-19 Restitution Assistance Fund for Victims of Securities Violations Act would create a fund at the Securities and Exchange Commission to provide restitution payments for

¹⁸ The "Senior Investor Pandemic and Fraud Protection Act" is directly modelled on precursor legislation that also aimed to make the necessary technical corrections to Section 989A, entitled the "The Empowering States to Protect Seniors from Bad Actors Act of 2019," which was proffered by the House Financial Services Committee in connection with a hearing on Consumer Financial Protection Bureau oversight in September 2019. The legislation is supported by a diverse coalition of organizations, including The Consumer Federation of America, The Insured Retirement Institute, The American Council of Life Insurers, The National Association of Insurance Financial Advisors, The American Association of Life Underwriters, The Financial Services Institute, The National Conference of Insurance Legislators, The Financial Planners Association, National Association of Personal Financial Planners, and The Certified Financial Planners-Board of Standards.

¹⁹ Among the entities that would be eligible to apply for the Senior Investor Protection grants established by the bill are state securities regulators, state insurance regulators, and certain state consumer financial product regulators.

²⁰ The legislation is also supported by the National Association of Insurance Commissioners ("NAIC").

²¹ See: NASAA's Legislative Agenda for the 116th Congress (April, 2019), accessible at <https://www.nasaa.org/wp-content/uploads/2019/03/NASAA-Legislative-Agenda-for-116th-Congress.pdf>.

²² Almost one in five Americans over the age of 65, which is nearly seven million seniors, have "been taken advantage of financially in terms of an inappropriate investment, unreasonably high fees for financial services, or outright fraud," according to a major survey conducted by Public Policy Polling (PPP) and the Investor Protection Trust (ITP). Additional information on the Elder Investment Fraud and Financial Exploitation Survey is accessible at: http://www.investorprotection.org/downloads/EIFFE_Survey_Report.pdf.

²³ The CFPB has stated the failure to implement Section 989A as directed is due to ambiguity regarding the Bureau's authority to fund the grants. See Letter from CFPB Director Richard Cordray to Senator Collins (August 14, 2014). ("While Section 989A(h) authorizes...there has been no appropriation made for these grants to date.")

individuals in connection with securities fraud related to coronavirus if they do not otherwise receive full payment of restitution.

NASAA wholeheartedly shares Congress's interest in the potential establishment of a nationwide investor restitution fund to help victims of investment fraud recover a portion of what they lost when full restitution is not possible. In many cases of investment fraud, some or all the money defrauded from investors may be already gone by the time the scam artist is caught and prosecuted. All too often, the victims of these investment scams are senior citizens who do not have the time and resources to recover from the losses that have been inflicted upon them. The establishment of a restitution fund to help qualifying investors recover a portion of their losses is a common-sense tool that can provide critical assistance to harmed investors, while also contributing to investor confidence broadly.

In fact, some states have already enacted and successfully implemented this type of legislation. Indiana and Montana have reported that their restitution assistance programs are successful. Since the inception of their funds, Indiana has paid approximately \$1 million in restitution assistance awards to 102 claimants, and Montana has paid \$1.6 million to 118 claimants. The average recipient was 64 years old in Indiana, and 82% of recipients were over 60 years old in Montana.

V. Conclusion

State securities regulators are standing on the front lines in the fight against the criminals and opportunists looking to abuse America's investing public. The pandemic has sadly heightened their vigor, as bad actors attempt to exploit a pandemic and the present economic disruption. NASAA and Congress share a compelling interest in protecting investors, punishing fraudsters, and contributing to a robust economic recovery.

Thank you for the opportunity to testify before the Subcommittee. I will be pleased to answer any questions you may have.



June 16, 2020

The Honorable Emanuel Cleavers
Chairman
House Committee on Financial Services
Subcommittee on National Security
2129 Rayburn House Office Building
Washington, DC 20515

The Honorable French Hill
Ranking Member
House Committee on Financial Services
Subcommittee on National Security
2129 Rayburn House Office Building
Washington, DC 20515

Re: "Senior Investor Pandemic and Fraud Protection Act" (Discussion Draft)

Dear Chair Cleavers and Ranking Member Hill:

Americans for Financial Reform writes to express support for the "Senior Investor Pandemic and Fraud Protection Act" (also known as the "Empowering States to Protect Seniors from Bad Actors Act"). This legislation is noticed for discussion as part of the "Cybercriminals and Fraudsters: How Bad Actors Are Exploiting the Financial System During the COVID-19 Pandemic" hearing in the Subcommittee on National Security, International Development and Monetary Policy today. The draft bill would enhance the ability of state regulators to protect seniors from financial exploitation by clarifying the funding mechanism for the program and ensuring that it does not compete with other CFPB funding needs.

The step is particularly timely now as seniors and vulnerable adults are increasingly being targeted by opportunistic scammers that prey on the confusion and fear of the COVID-19 pandemic. Congress has repeatedly recognized that seniors are especially susceptible to fraud and agree on a bipartisan basis regarding the need to enhance resources to educate and protect senior investors. Congress has also recognized that state regulators are an essential part of the effort to combat senior financial exploitation because they serve on the front lines and are often the first to respond to those affected.

We support the proposed legislation that would implement a targeted retail investor protection program, which was originally envisioned and authorized by Section 989(A) of the Dodd-Frank Act, but never put into effect. The "Senior Investor Pandemic and Fraud Protection Act" will enable qualifying states and state regulators to receive up to \$500,000 annually in grant funding to combat financial fraud of seniors and vulnerable adults for a maximum of 2 consecutive years, for a total of \$1 million. State regulators will be able to use the funds for such purposes as hiring staff to investigate cases involving fraudulent marketing, funding technology, equipment, and training for prosecutors to increase the prosecution of salespersons who target seniors and vulnerable adults, and providing educational materials to seniors and vulnerable adults to raise awareness of misleading or fraudulent marketing.

As we continue to battle the COVID-19 pandemic, we ask Congress to provide state financial regulators with the tools necessary to effectively combat financial exploitation of those most vulnerable during this crisis and ensure that their savings are financially protected during this uncertain time.

Sincerely,

Americans for Financial Reform

1615 L Street NW, Suite 450, Washington, DC 20036 | 202.466.1885 | ourfinancialsecurity.org



3138 10th Street North
Arlington, VA 22201-2149
703.522.4770 | 800.336.4644
f: 703.524.1082
nafcu@nafcu.org | nafcu.org

National Association of Federally-Insured Credit Unions

June 15, 2020

The Honorable Emanuel Cleaver
Chairman
Subcommittee on National Security,
International Development and
Monetary Policy
Committee on Financial Services
U.S. House of Representatives
Washington, DC 20515

The Honorable French Hill
Ranking Member
Subcommittee on National Security,
International Development and
Monetary Policy
Committee on Financial Services
U.S. House of Representatives
Washington, DC 20515

Re: Tomorrow's Hearing, "Cybercriminals and Fraudsters: How Bad Actors Are Exploiting the Financial System During the COVID-19 Pandemic"

Dear Chairman Cleaver and Ranking Member Hill:

I am writing on behalf of the National Association of Federally-Insured Credit Unions (NAFCU) to share our thoughts ahead of tomorrow's virtual hearing entitled, "Cybercriminals and Fraudsters: How Bad Actors Are Exploiting the Financial System During the COVID-19 Pandemic." NAFCU advocates for all federally-insured not-for-profit credit unions that, in turn, serve 120 million consumers with personal and small business financial service products.

As we have shared with you previously, credit unions are keenly aware of the hardships their members are facing due to the COVID-19 pandemic and are working around the clock to proactively assist them. This assistance includes warning members about bad actors who will seek to commit fraud to take financial advantage of them. As you know, the pandemic has emboldened bad actors who are seeking to exploit fearful and anxious Americans, and it is vital that credit unions have the ability to alert their members to potential threats. NAFCU appreciates the Subcommittee's attention to this crisis and is supportive of efforts to combat cybercriminals who seek to take advantage of the current pandemic. Cybersecurity is a critical issue for credit unions – according to a 2019 NAFCU survey, credit unions report that the share of their overall budget devoted to cybersecurity has more than doubled over the past five years. Yet, there remain important issues that need to be addressed on this front, even outside of the pandemic. Congress taking action on these issues can help to mitigate Americans' risk of falling prey to fraudulent activity, both during this pandemic and beyond.

First, NAFCU believes there is an urgent need for a national data security standard for those who collect and store consumer information. While depository institutions have had a national standard on data security since the passage of the *Gramm-Leach-Bliley Act* (GLBA) over two decades ago, other entities who handle consumer financial data may not be held to the same rigorous standards or subject to meaningful supervision. Along those same lines, we also believe that there is a need for a uniform national consumer data privacy standard as opposed to a patchwork of standards stemming from different state data privacy laws. Such a standard should recognize what has been

The Honorable Emanuel Cleaver, The Honorable French Hill
June 15, 2020
Page 2 of 2

in place and is working for consumers, credit unions and others under existing laws such as the GLBA. Our nation's current patchwork of data privacy and security laws contributes more to operational and administrative burden rather than the substantive protection of consumers. Furthermore, inconsistent rules can be exploited by bad actors. Although we have been calling on Congress to enact a national standard for years, we believe that action now is critical as more bad actors seek to exploit the current situation. We hope today's hearing can be another step toward achieving these goals.

Second, we believe that the *Bank Secrecy Act* (BSA)/Anti-Money Laundering (AML) system is in need of improvements and reform. NAFCU has consistently recognized the importance of the Financial Crimes Enforcement Network (FinCEN) and BSA/AML requirements in assisting in the prevention of tax evasion, money laundering and terrorist financing. Credit unions support efforts to combat criminal activity in the financial system. Our members have a good working relationship with FinCEN, and they consistently inform us that the publication of periodic BSA/AML guidance is very helpful. However, BSA/AML requirements remain a burden to implement, and we believe that the system is in need of modernization, especially considering the increase in fraud and illicit financial activity during this pandemic. This includes beneficial ownership reform, which is more critical now than ever. We were pleased to see the House pass H.R. 2513, the *Corporate Transparency Act of 2019*, and H.R. 2514, the *COUNTER Act of 2019*, last fall that would help strengthen and improve the BSA/AML system, and we urge you to work with your colleagues in the Senate so that this legislation becomes law.

We thank you for your leadership and ongoing efforts to support American consumers and financial institutions during these uncertain times. We appreciate the opportunity to share our input and look forward to continuing to work with the Subcommittee on these issues. Should you have any questions or require any additional information, please contact me or Sarah Jacobs, NAFCU's Associate Director of Legislative Affairs, at (571) 289-7550.

Sincerely,



Brad Thaler
Vice President of Legislative Affairs

cc: Members of the Subcommittee on National Security, International Development and Monetary Policy

Submission for the Record**Ms. Mieke Eoyang****Vice President for the National Security Program****Third Way**

I'd like to start by commending the Chair, Ranking Member, and members of the subcommittee for focusing its attention on this important issue. Cybercrime has been on the rise globally over the past decade, but the onset of the COVID-19 Pandemic has caused an increase in cybercrime, as criminals, like others, work from home, and prey upon the anxieties and fears of the population.

It is an honor to submit this statement and accompanying report to the record.

COVID-19 is exacerbating a cybercrime crisis that already existed.

We have long known that cybercrime is on the rise. As Americans and others around the world increase their reliance on technology for communications, commerce, banking, and even building connections to others, the internet becomes a more attractive target for criminals to prey upon their victims.

A rising and often unseen crime wave is mushrooming in America. There have been approximately 340,000 cybercrime incidents reported to the FBI each year from 2015-2019, with the number of reports increasing each year.¹ While the FBI estimates that only one in six victims reports their incidents to the FBI, Third Way's analysis indicates that this figure is off by an order of magnitude.² Public polling by both Gallup and Third Way indicates that one in four Americans has been victimized by cybercrime, which would suggest that the true level of incidents is around 30 million, over 100 times higher than what the FBI is seeing.³ If these polls accurately reflect what is happening to Americans, cybercrime is the most prevalent form of crime in America.

Even before this pandemic, the costs of cybercrime were enormous. The White House Council of Economic Advisers estimated in 2016 that malicious cyber activity costs the U.S. economy up to \$109 billion annually and these costs are increasing.⁴ Global estimates are even higher, with some saying cybercrime will cost the world in excess of \$6 trillion annually by 2021, up from \$3 trillion in 2015.⁵

Unfortunately, the COVID-19 pandemic has seen a spike in cybercrime from an already high baseline. Speaking in an online panel hosted by the Aspen Institute, FBI Deputy Assistant Director Tonya Ugoretz said the number of reports has up to quadrupled compared to months before the pandemic.

"The FBI has an Internet Crime Complaint Center, the IC3, which is our main ingest point. Sadly the IC3 has been incredibly busy over the past few months," Ugoretz said.

"Whereas they might typically receive 1,000 complaints a day through their internet portal, they're now receiving something like 3,000 - 4,000 complaints a day not all of those are COVID-related, but a good number of those are."⁶

Not only are cybercriminals looking to exploit the pandemic for financial gain, but nation-states are also turning to cybercrime and seeking out cybercrime tools to steal intelligence about America's response to COVID-19.⁷ There are continued reports of cybercriminals stealing stimulus payments in the midst of what has been one of the greatest times of economic hardship for many Americans.⁸ Some estimates are that the financial services sector in the United States saw an increase of 38% from February 2020 to March 2020 in cybercrime as the COVID-19 Pandemic particularly hit the country.⁹ The Secret Service estimates that \$30 billion of the coronavirus stimulus funding will be stolen.¹⁰ The targeting of hospitals and vaccine development labs in the United States and around the globe by malicious cyber actors during the pandemic is also particularly appalling.

Unfortunately, criminal prosecution is all too rare in cybercrime.

Reflecting on the cybersecurity debate, most of the policy discussions, particularly on Capitol Hill, largely focus on prevention – on strengthening and defending the systems that we use every day. Unfortunately, defending the systems alone will not solve the problem. For every security flaw that gets fixed, the cybercriminals are at large to find another. Right now, the perpetrators of these attacks operate with pure impunity because there have rarely been any consequences for their actions. Based on Third Way's analysis of government data, less than 3 in 1000 reported cyber incidents see an arrest.¹¹ By contrast, in 2018, 45.5 percent of violent crimes and 17.6 percent of property crimes were cleared.¹² This makes cybercrime one of the least likely crimes in America to result in justice against the perpetrators.

There are many reasons why the cybercrime enforcement rate is low. Cases are complex. All too often the perpetrator and the victim are unknown to each other and can be on opposite sides of the globe. Law enforcement does not have sufficient numbers of trained or technical personnel to pursue the overwhelming number of cases.¹³ Cybercriminals often operate in countries that either lack the will or the capability to investigate and prosecute them.¹⁴ Cases involving victims in multiple jurisdictions and networks operating across national boundaries requires coordination that is often lacking.¹⁵ This may be particularly true when we talk about public sector cooperation with the private sector where trust is often absent.¹⁶

But it is not enough to throw up our hands in futility at the complexity of the cases, denying the victims justice. Cybercrime is the most prevalent type of crime with the lowest enforcement rate. We can and must identify reforms and solutions to address this crime. As crime moves off the streets and onto the internet, law enforcement, backed by strong civil liberties protections, must follow.

To Catch a Hacker report makes recommendations for a comprehensive approach against cybercrime.

Third Way's report, To Catch A Hacker, takes a comprehensive look at cybercrime, the challenges to enforcement, and identifies particular areas for reform. We submit the report with this testimony for the subcommittees' review.

Thank you for the opportunity to submit this testimony.

¹ Internet Crime Complaint Center. "2019 Internet Crime Report." *Federal Bureau of Investigation*, 11 Feb. 2020, pp. 5, https://pdf.ic3.gov/2019_IC3Report.pdf. Accessed 9 June 2020.

² Wexler, Chuck. "New National Commitment Required: The Changing Nature of Crime and Criminal Investigations." *Police Executive Research Forum*, Jan. 2018, pp. 5, <https://www.policeforum.org/assets/ChangingNatureofCrime.pdf>. Accessed 9 June 2020.

³ Reinhart, RJ. "One in Four Americans Have Experienced Cybercrime." *Gallup.com*, Gallup, 10 Dec. 2018, <https://news.gallup.com/poll/245336/one-four-americans-experienced-cybercrime.aspx>. Accessed 9 June 2020.

⁴ United States White House, The Council of Economic Advisers. "The Cost of Malicious Cyber Activity to the US Economy." Feb. 2018, pp. 1, <https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf>. Accessed 9 June 2020.

⁵ Morgan, Steve. "2019 Official Annual Cybercrime Report." *Herjavec Group*, Dec. 2018, pp. 2, <https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf>. Accessed 9 June 2020.

⁶ Cimpanu, Catalin. "FBI says cybercrime reports quadrupled during COVID-19 pandemic." *Zdnet.com*, 18 Apr. 2020, <https://www.zdnet.com/article/fbi-says-cybercrime-reports-quadrupled-during-covid-19-pandemic/>. Accessed 9 June 2020.

⁷ FBI and CISA. "People's Republic of China (PRC) Targeting of COVID-19 Research Organizations." Public Service Announcement. 13 May 2020, https://www.cisa.gov/sites/default/files/publications/Joint_FBI-CISA_PSA_PRC_Targeting_of_COVID-19_Research_Organizations_S508C.pdf. Accessed 9 June 2020.

⁸ <https://www.secureworks.com/blog/cybercriminals-target-us-citizens-for-covid-19-stimulus-fraud>
⁹ Scroton, Alex. "Coronavirus: Cyber attacks on banks seen spiking, says Carbon Black." *Computerweekly.com*, 16 Apr. 2020, <https://www.computerweekly.com/news/252481684/Coronavirus-Cyber-attacks-on-banks-seen-spiking-says-Carbon-Black>. Accessed 9 June 2020.

¹⁰ Michael D'Ambrosio. "Prepared Testimony on 'COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic'." Testimony for the Senate Committee of the Judiciary, 9 June 2020, pp. 3, <https://www.judiciary.senate.gov/imo/media/doc/D'Ambrosio%20Testimony.pdf>. Accessed 10 June 2020.

¹¹ Peters, Allison and Ishan Mehta. "This is not the time to leave our hospitals unprotected against cyberattacks." *The Washington Post*, 19 Mar. 2020, <https://www.washingtonpost.com/opinions/2020/03/19/this-is-not-time-leave-our-hospitals-unprotected-against-cyberattacks/>. Accessed 8 June 2020.

¹² Federal Bureau of Investigations, Uniform Crime Reporting Program. "Clearances." 2018 Crime in the United States, *Criminal Justice Information Services Division*, <https://ucr.fbi.gov/crime-in-the-u.s/2018/crime-in-the-u.s.-2018/topic-pages/clearances>. Accessed 9 June 2020.

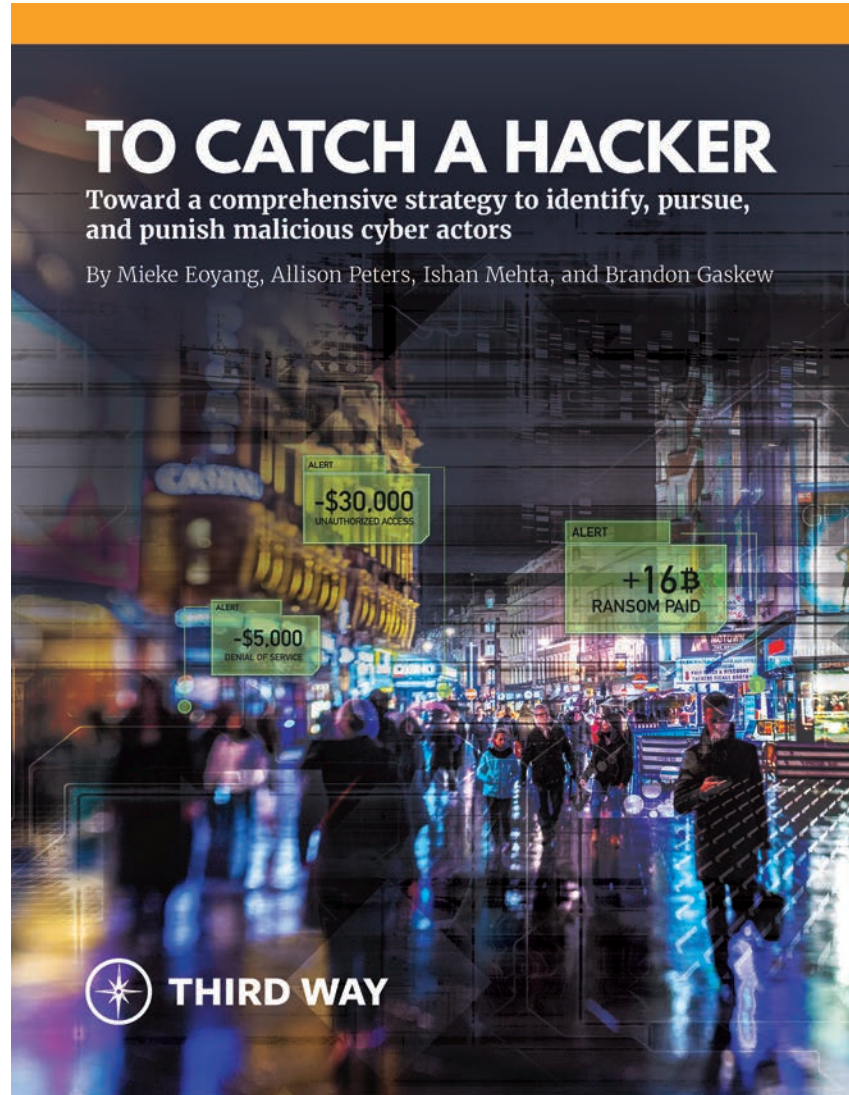
¹³ Carter, William A, and Jennifer C Daskal. "Low-Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge." *Center for Strategic and International Studies*, July 2018, pp. 15-16. csis-prod.s3.amazonaws.com/s3fs-public/publication/180725_Carter_DigitalEvidence.pdf?tAGR_DvxRdp0RspiGYNGcGKTUjrGY3rN. Accessed 9 June 2020.

¹⁴ Peters, Allison and Amy Jordan. "Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime." *Journal of National Security Law and Policy*, Vol. 10, No. 3, 2 Oct. 2019, pp. 492. <https://thirdway.imgix.net/pdfs/override/Countering-the-Cyber-Enforcement-Gap-Strengthening-Global-Capacity-on-Cybercrime.pdf>. Accessed 9 June 2020.

¹⁵ Peters, Allison and Amy Jordan. "Countering the Cyber Enforcement Gap:

Strengthening Global Capacity on Cybercrime." *Journal of National Security Law and Policy*, Vol. 10, No. 3, 2 Oct. 2019, pp. 494. <https://thirdway.imgix.net/pdfs/override/Countering-the-Cyber-Enforcement-Gap-Strengthening-Global-Capacity-on-Cybercrime.pdf>. Accessed 9 June 2020.

¹⁶ Germano, Judith H. "Cybersecurity Partnerships: A New Era of Public Private Collaboration." *The Center on Law and Security*, NYU School of Law, Oct. 2014, pp. 3-6, <https://www.lawandsecurity.org/wp-content/uploads/2016/08/Cybersecurity.Partnerships-1.pdf>. Accessed 9 June 2020.





Acknowledgments

We would like to acknowledge and thank the many people who have contributed to this report and shared their perspectives on the cyber enforcement gap. The support, expertise, and guidance that has been provided to us has been invaluable in steering the direction of this report.

In particular, we would like to thank our former fellows Jayati Dev and Adam Twardowski for their incredible research support without which this report would not be possible. We would also like to thank Third Way's Founders Jim Kessler and Jonathan Cowan for their endless support and strategic guidance.

Additionally, we are grateful to the members of the Advisory Board of Third Way's Cyber Enforcement Initiative for their continued inputs and support. Each brings a wealth of diverse experience and expertise to the Advisory Board and we are thankful for their partnership. However, the views expressed in this paper should be viewed as the authors' alone and not presumed to be endorsed by the Cyber Enforcement Initiative's Advisory Board:

Gina Abercrombie- Winstanley	Mary DeRosa	Chan Park
James Baker	Judith Germano	Gregory Rattray
Cassandra Chandler	Orin Kerr	Paul Rosenzweig
Jennifer Daskal	Andrew McLaughlin	Ari Schwartz
Rajesh De	Christopher Painter	Ben Wittes

Finally, we would like to thank the many individuals we have spoken to throughout the development of the Third Way Cyber Enforcement Initiative who have provided critical ideas, data, and feedback to us. In particular, we are grateful to Eli Sugarman, Michael Woods, Taxpayers for Common Sense, the Consumer Bankers Association, Kathryn Rosen, Matthew Waxman, Jonah Force Hill, Kevin Bankston, Joshua Alexander, David Lieber, Jeff Ratner, Bruce Schneier, Suzanne Spaulding, Matt Tait, Allan Friedman, and Jing de Jong-Chen. We are thankful to the many other representatives of industry and civil society groups who have provided us with their thoughts on this Initiative.

To Catch a Hacker: Policy Recommendations

Cybercriminals operate with a sense of impunity as only 0.3% of malicious cyber incidents see an arrest, according to our analysis of FBI reported data. What that means is that the United States is facing a massive cyber enforcement gap just as the cybercrime wave continues and malicious cyber activity that threatens our national security is becoming more common. To close the cyber enforcement gap, we call for a comprehensive, strategic approach to identify, stop, and punish malicious cyber actors. The US maintains robust efforts to secure existing computer networks, but heavily relying on air tight systems and mistake-less human users can only accomplish so much. In our new paper, we call for ten US policy actions (some that build off existing efforts) that can form the contours of such a strategy to go after human attackers.

Domestic Enforcement Reform

1. **A Larger Role for Law Enforcement:** Strengthen capacity building efforts so that law enforcement, enabled by diplomacy, can target the humans behind cyberattacks.
2. **A Cyber Enforcement Cadre:** Address not only workforce shortages, but the way the cyber enforcement workforce is trained, incentivized, and retained.
3. **Better Attribution Efforts:** Increase investments in research and development for attribution technology, better digital forensics, and prioritize efforts to build international alliances that improve timeliness and impact of attribution efforts.
4. **A Carrot and Stick Approach to Fugitives:** Adopt a broader reward-based system to incentivize information sharing that can lead to arrests of malicious cyber actors balanced with the smart use of targeted sanctions.

International Cooperation and Coordination Reform

5. **An Ambassador-level Cyber Quarterback:** Institute an ambassador-level cyber coordinator position at the State Department with a clear mandate and resources on cyber enforcement.

Stronger Tools in the Diplomacy Arsenal:

Expand the number and streamline processes for agreements with other countries that help bring cyber attackers to justice and continue to utilize the multilateral Budapest Convention.

7. **Better International Capacity for Enforcement:** Support efforts to build the capacity of other countries on cybercrime investigations, while ensuring cybercrime and cybersecurity efforts are not used to suppress civil liberties and human rights.

Structural and Process Reform

8. **Better Success Metrics:** Establish mechanisms to measure the scope of the cyber enforcement problem and the effectiveness of government efforts.
9. **Organizational Changes and Interagency Cooperation:** Evaluate further needed policy changes to de-conflict the missions of the agencies responsible for cyber enforcement.
10. **Centralized Strategic Planning:** Institute an overarching, comprehensive strategy for US cyber enforcement led by a senior official at the White House.

The lack of an overarching strategy to deal with this growing threat is ominously analogous to the pre-9/11 US government approach to terrorism. We need a strategy that doesn't just focus on building a better safe, but focuses on catching the safecracker.

To Catch a Hacker:

Toward a comprehensive strategy to identify, pursue, and punish malicious cyber actors

By Mieke Eoyang, Allison Peters, Ishan Mehta, and Brandon Gaskew

Introduction

On February 21, 2018, computer monitors in Colorado's Department of Transportation went gray. In simple red and black text, an ominous message: "All your files are encrypted." For three bitcoin, or what was then \$27,000, the department could have the decryption keys.¹ They refused.² Soon after, the department lost use of 150 servers and shut down 2,000 employee computers.³ Two weeks later the department was hit a second time, by another strain of the same ransomware, hampering already costly recovery efforts.⁴ One month following this attack, Atlanta's municipal computer systems came to a slow crawl. Again, a message appeared on the city's network demanding ransom in exchange for the decryption of their files. One-third of all city services were sidelined and critical data, including police files and evidence, was lost.⁵ In Indiana this past January, the Hancock Health Hospital system was hit with the same type of ransomware. The attackers took hostage of more than 1,400 files on their networks, which included medical records of current patients, only releasing them once a ransom was paid.⁶

Each of these incidents were part of the same ransomware attack known as SamSam. SamSam may be thought of as just a series of ones and zeroes but behind SamSam is a person or a set of people. They could be a member of a terrorist group, a criminal organization, or an agent of a nation-state, seeking to exploit computer vulnerabilities to advance their agenda. They may simply be a cyber thief – finding clever ways of breaking into systems and collecting ransoms through hard-to-trace cryptocurrencies. But whoever it is they have collected payments totaling an estimated \$6 million since 2015,⁷ and they have cost their victims even more millions of dollars in recovery costs. Atlanta alone could reportedly spend \$17 million in incident response and mitigation.⁸ This attack was technically sophisticated, both in its invasion and its execution, and hit victims across many different jurisdictions. The person or persons behind SamSam are still at large, and as this report will show, it is safe to assume that they believe they will never be caught. This must change.

In this paper, we argue that the United States currently lacks a comprehensive overarching strategic approach to identify, stop and punish cyberattackers. We show that:

1. **There is a burgeoning cybercrime wave:** A rising and often unseen crime wave is mushrooming in America. There are approximately 300,000 reported malicious cyber incidents per year, including up to 194,000 that could credibly be called individual or system-wide breaches or attempted breaches.⁹ This is likely a vast undercount since many victims don't report break-ins to begin with.¹⁰ Attacks cost the US economy anywhere from \$57 billion to \$109 billion annually and these costs are increasing.¹¹
2. **There is a stunning cyber enforcement gap:** Our analysis of publicly available data shows that cybercriminals can operate with near impunity compared to

their real-world counterparts. We estimate that cyber enforcement efforts are so scattered that less than 1% of malicious cyber incidents see an enforcement action taken against the attackers.

3. **There is no comprehensive US cyber enforcement strategy aimed at the human attacker:** Despite the recent release of the *National Cyber Strategy*, the United States still lacks a comprehensive strategic approach to how it identifies, pursues, and punishes malicious human cyberattackers and the organizations and countries often behind them. We believe that the United States is as far from this human attacker strategy as the nation was toward a strategic approach to countering terrorism in the weeks and months before 9/11.

In order to close the cyber enforcement gap, we argue for a comprehensive enforcement strategy that makes a fundamental rebalance in US cybersecurity policies: from a heavy focus on building better cyber defenses against intrusion to also waging a more robust effort at going after human attackers. We call for ten US policy actions that could form the contours of a comprehensive enforcement strategy to better identify, pursue and bring to justice malicious cyber actors that include building up law enforcement, enhancing diplomatic efforts, and developing a measurable strategic plan to do so.

This rebalance can only be achieved if we increase the emphasis on, and resources in, US cybersecurity efforts to include a greater focus on identifying, stopping, and punishing the human attacker. This means:

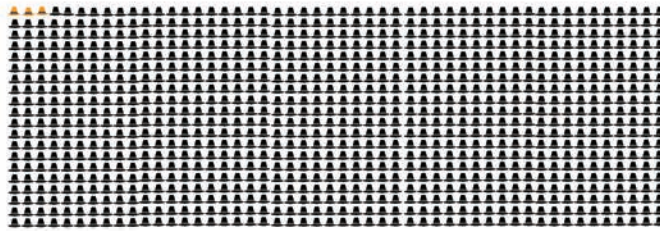
- Shedding a blame-the-victim mentality that drives the defensive approach in favor of one of shared responsibility that invigorates a catch-the-hacker approach, and
- Creating a more balanced approach that places more emphasis on law enforcement and diplomacy to prevent an overreliance on the military.

SamSam is only one of thousands of attacks affecting Americans, and it is just a matter of time before another malicious actor aims at bigger targets for reasons far more nefarious than SamSam. While system and network owners and operators have obligations to provide the best security they can, we have seen time after time that a determined attacker will eventually get through. By putting the human attacker in the crosshairs of America's cybersecurity efforts we can instead raise the costs of their actions to not only bring attackers to justice, but also to deter future attacks—whether they come from criminals, organizations, or hostile governments.

The Enforcement Gap and the Burgeoning Cybercrime Wave

Calculating the scope of the cyber enforcement gap is a challenging if not impossible task due to the lack of comprehensive public data across agencies. Based on our analysis of the publicly available data that does exist from federal, state, and local sources, we estimate the chance of arresting a cybercriminal is less than 1% of the total number of malicious cyber incidents reported annually to the federal government. We define this enforcement rate as the ratio of arrests to the number of incidents reported, as data on indictments and prosecutions is not consistently reported at all levels. In other words, this enforcement rate may be optimistic as arrests do not mean conviction.

Only 3 in 1,000 cyber incidents see an arrest



Note: every "black hat" represents one cyber incident

By comparison, the clearance rate for property crimes was approximately 18% and for violent crimes 46%, according to the Federal Bureau of Investigation's (FBI) Uniform Crime Report (UCR) for 2016. The clearance rate is the number of cases where at least one person has been arrested, charged with the commission of an offense, and referred for prosecution.¹² Those numbers in comparison to a less than 1% rate for just arrests for computer crimes is a drastic difference in the rate of enforcement.

What happens when there is a criminal, terrorist, or other malicious actor engaging in destabilizing activity in which the likelihood of getting caught and punished is close to zero? In this section, we lay out some of the dimensions of the cybercrime wave in the United States and globally. The burgeoning cybercrime wave is the result of both the ubiquity of technology and the one-sided nature of our defenses: a reliance on building systems that are harder and harder to breach, training lay users to be harder and harder to fool, and faced with hackers who are harder and harder to catch.

Malicious cyber actors are rarely caught and the effort to do so is uncoordinated, under-resourced, and under-prioritized.

The ubiquity of technology means every critical infrastructure sector in the United States—from nuclear power plants to water facilities—utilizes some form of computer-enabled system for their operations that, if attacked successfully, could have devastating impacts on Americans. That is why the US Department of Treasury has designated cybersecurity incidents as one of the biggest threats to the stability of the entire US financial system.¹³

Nearly every US citizen's personal, financial, and sensitive information is stored on a connected device in some form. There are now more active mobile phones, which store sensitive information on them, than the number of people on the planet, and Cisco predicts 27.1 billion up from 17.1 billion in 2016 connected devices by 2021 or roughly 3.5 per person.¹⁴ Each device is

potentially an attack vector that a malicious actor could exploit. Each device has applications, operating systems, and network connections, which all have potential vulnerabilities for an attacker to exploit.

And as we discovered and noted above, the effort to catch malicious cyber actors is uncoordinated, under-resourced, and under-prioritized— just a handful of reasons why those actors are rarely caught.

The Cybercrime Wave

There's a rising and often unseen crime wave happening in America. The FBI received 298,728 self-reported cybercrime complaints in the United States in the year 2016 alone through its Internet Crime Complaint Center (IC3).¹⁵ Of those, as many as 193,700 cybercrimes could credibly be described as serious attempts at individual or systemic cyber breaches, including such activities as identity theft (16,878 reported incidents), personal data breach (27,573), ransomware (2,673), and malware (2,783), according to the IC3 database.¹⁶ This is only part of the picture, as the FBI estimates that fraud victims report only 15 percent of crime nationwide to law enforcement.¹⁷ That may mean there are 2 million cybercrimes per year, or roughly equal to 1.4 million burglaries in a given year, if underreporting estimates are accurate.¹⁸

The IC3 is an FBI center established in May 2000 to serve as a central hub for Internet crime victims to alert federal, state, and local authorities to suspected criminal Internet activity.¹⁹ From 2013 to 2017, the IC3 has received over 1.4 million complaints.²⁰ While IC3's methodology tabulates each individual's complaint as a separate entry, the Verizon Data Breach Investigations Report states that there have been over 53,000 incidents targeted at organizations.²¹ And America isn't alone. The International Police Organization (INTERPOL), the multilateral organization that facilitates global law enforcement cooperation to fight international crime, states that cybercrime is one of the fastest growing areas of crime.²²

What do we mean by “cybercrime?”

While this paper refers to the more general term “malicious cyber activity” in certain places, or “cyberattack” for high-impact incidents, we're primarily focused on cybercrime or crimes that use or target computer networks. This includes data theft, fraud, distributed denial-of-service (DDoS) attacks, worms, ransomware, and viruses.²³ We recognize the concerns raised with the term “cyberattack,”²⁴ but considering its widespread adoption and lack of global consensus on overall terminology, we continue its use in certain places to describe significant cyber incidents.

Cybercriminals come in all shapes and sizes. The FBI assesses that these threats can come from attackers with a host of different motivations and affiliations.²⁵ High-level intrusions usually stem from attackers affiliated with global organized crime syndicates or state-sponsored attackers.²⁶ Hacker-rings or lone actors typically run mid-level identity fraud or carding schemes for financial gain.²⁷ Finally, privacy crimes, such as doxing, are targeted crimes usually committed by lone actors with malicious personal or political motivation.²⁸

However, that landscape is changing fast. Nation-states like North Korea have attacked systems for a variety of reasons. Sony was hacked to prevent reputational harm, the Bank of Bangladesh heist was for financial gain, and the WannaCry attack was motivated by a desire to cause economic chaos.²⁹ Terrorists have also continued to use the Internet as a key operational tool, including launching malicious cyberattacks against targets in the United States.³⁰ Many of these crimes threaten the stability of systems, either intentionally or through the way they spread.

There are also a few categories of malicious cyber activity that, while extremely serious, do not threaten to disrupt the stability of systems. While critically important, our recommendations will not focus on what the Department of Justice refers to as “cyber-enabling crimes threatening personal privacy,” such as cyber-enabled stalking, non-consensual pornography, and cyber-enabled harassment.³¹ The recommendations also do not cover issues related to child pornography. These devastating crimes involve potentially very different motivations than other forms of cybercrime and deserve dedicated research related to government responses to these crimes.

The rewards from a successful cyberattack are high, and the costs (in terms of risk) low, which has incentivized malicious actors to develop more effective hacking techniques. Some examples of those techniques and their costs are as follows:

- Ransomware attacks, where an attacker encrypts the victim's data and typically only frees it when a ransom is paid, doubled in frequency between 2016 and 2017 with incidents affecting a diversity of targets and disrupting the operations of public services and large corporations around the country and globe.³²
- Malware attacks on mobile devices have now surged with an increase in 54% globally from 2016 to 2017.³³
- Software update supply chain attacks in which malware is implanted into software packages to infect computer systems has increased by 200 percent globally in 2017 from the year prior.³⁴
- The Ponemon Institute estimates the average total cost of a data breach at \$3.62 million.³⁵
- IC3 calculated that reported crimes, such as identity theft and online fraud, cost victims more than \$1.42 billion.³⁶
- In 2016, the White House Council of Economic Advisors estimated in 2016 that malicious cyber activity costs the United States economy between \$57 billion and \$109 billion per year.³⁷ Other estimates put the number as high as \$3 trillion for the global economy annually.³⁸

The targets that malicious cyber actors are hitting with their attacks span a wide spectrum of sectors with the healthcare, public, accommodation, and manufacturing bearing the brunt of security incidences and data breaches.³⁹ For example, the Mirai Botnet attack in October 2016 led to some of the world's most popular websites going offline for up to twelve hours—including

Netflix, Twitter, Reddit, PayPal, The New York Times, and The Wall Street Journal—costing these companies millions of dollars in lost revenue.⁴⁰

Criminal use of technology is creating entirely new categories of crime that never existed before the digital age.⁴¹ It is ending the notion of “good neighborhoods” and “bad neighborhoods” when it comes to crime because cyberspace is both ubiquitous and borderless. New types of crime from carding schemes, to ransomware, to crypto mining have made investigations even more complex where the victim and perpetrator may be unknown to each other and may be in different countries. Technologies like Virtual Private Networks (VPNs), the Tor browser,⁴² and cryptocurrencies like Bitcoin lend anonymity, or at least perceived anonymity, to the malicious cyber actor.

These technologies also help make attacks more effective and easier to execute. Tools created using machine learning allow malicious cyber actors to perform reconnaissance, or information-gathering efforts, more efficiently and to a much higher degree of accuracy. For attackers, the more information they have about the systems and the operators of the system, the more effective the attack. Attackers can assess information regarding potential vulnerabilities, unpatched systems, and exploits much quicker through the advanced technology available to them. Marketplaces and discussion forums on the dark web have made buying and using cyber-exploits as easy as shopping for shoes online.⁴³

Cybercrime has hit victims across the United States in every single state and territory. California, Florida, Texas, New York, and Pennsylvania—states with very different demographics, corporate representation, and cybersecurity laws—make up the highest number of victims.⁴⁴ These states have been hit by devastating economic losses as a result of the cybercrime wave.⁴⁵

Cybercrime's impact is so broad that it has security implications for the entire nation and globe. A single incident like the WannaCry cyberattack in 2017 affected more than 200,000 computer systems in 150 countries and potentially cost the world economy \$4 billion.⁴⁶ Malicious cyber actors have attacked health care systems and critical infrastructure in the United States, such as Industrial Control Systems (ICS), the electric grid, and dams. A successful attack executed on these systems can threaten life, property and cause large scale destruction. In March of this year, the Department of Homeland Security (DHS) and the FBI issued an alert that the Russian government was targeting the electric grid and other critical energy systems.⁴⁷ In 2015, malicious actors managed to access the ICS software at a water treatment plant and tampered with the controls related to water flow and the amount of chemicals used to treat the water.⁴⁸

The cybercrime wave is so big it should be setting off alarm bells at every level of law enforcement. And yet, the response from the enforcement community is a drop in the bucket compared to the sheer volume of crimes occurring.

Beyond financial harm, some cyberattackers, at the behest of nation states, are doing real damage to US national security. US defense contractors have become targets for adversaries seeking to steal national security secrets. Recently, Chinese government hackers infiltrated the network of a US Navy contractor, stealing data on undersea warfare and secret plans for US submarine anti-ship missiles.⁴⁹ China and others are hacking US companies to steal intellectual property, at an estimated cost of \$225 billion to \$600 billion annually.⁵⁰ Hostile nations are also using cyber operations to affect US national security personnel directly. In 2014 and 2015,

the Office of Personnel Management⁵¹ suffered a massive data breach exposing the sensitive information of up to 22 million people, including personal information in their security clearance forms. And, of greatest concern, Russia's malicious cyber activities aimed at trying to affect the outcome of the 2016 US presidential election have been well-documented in indictment after indictment.⁵²

The cybercrime wave is so big it should be setting off alarm bells at every level of law enforcement. And yet, the response from the enforcement community is a drop in the bucket compared to the sheer volume of crimes occurring.

The Enforcement Gap

We know how big the problem is, but assessing the adequacy of the response to the problem is tougher. Not only are we in a cybercrime wave, but we also have a hidden enforcement crisis.

Third Way's analysis estimates that the enforcement rate for reported incidents of the IC3 database is 0.3%. Taking into account that cybercrime victims often do not report cases, the effective enforcement rate estimate may be closer to 0.05%.

How did we calculate the cyber enforcement rate?

There were significant challenges to estimating an aggregate cyber enforcement rate for the purpose of this research. Most significantly, there are currently no public databases which specifically report enforcement metrics on computer crime across all localities in the same way that exists for other categories of crime. We analyzed close to two dozen public and private databases to calculate the cyber enforcement rate. There were numerous discrepancies and inconsistencies across the different datasets that estimated the number of cyber incidents. Additionally, none of the datasets had comprehensive attribution information. To calculate the enforcement rate, we therefore decided to use Department of Justice (DOJ), FBI, and Secret Service self-reported numbers on incidents and arrests. This data is not perfect and includes categories of crimes that we do not directly address in our recommendations, such as privacy crimes, and the number of incidents relies on reports by victims to the federal government. Yet, these are the best datasets publicly available that give a picture of the enforcement gap rate for the United States. This is precisely why we call for better comprehensive reporting in our recommendations later in this report.

The FBI IC3 received 298,728 complaints in 2016.⁵³ By analyzing a variety of official US government reporting databases, we determined that there were fewer than 1,000 arrests that year between federal, state, and local law enforcement agencies for reported cybercrimes.

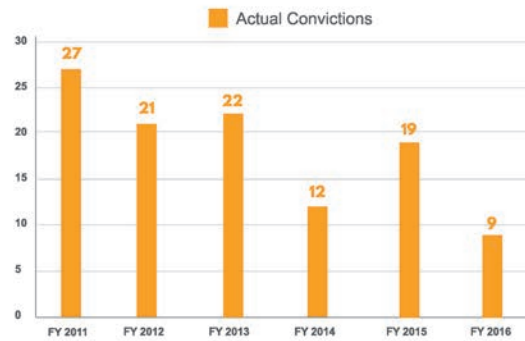
Specifically, to determine the number of enforcement actions we looked at various reports of the number of cybercrime arrests. In 2014 and 2015, through the FBI's Uniform Crime Reporting (UCR) Program, the Bureau reported the number of individuals arrested for "criminal computer intrusion" by each FBI field office. The total number was 105 for 2014 and 49 for 2015.⁵⁴ In 2016, UCR transferred to

the National Incident-Based Reporting System (NIBRS) and no longer separates out the arrest numbers for computer crime in their reporting. However, in 2016, the arrest numbers for computer crime by state and local law enforcement were included through NIBRS for the first time. The number reported under “hacking/ computer invasion” crime was 581 for 2016, the most recent year reported, which includes reporting from 6,849 state and local agencies.⁵⁵ The Secret Service reported 251 cybercrime arrests in 2016.⁵⁶ If we assume the FBI field offices made a similar number of arrests as in the previous two years in 2016 combined, we arrive at the total federal, state, and local computer crime arrests to be between 871 and 927 for 2016, barring a significant increase in federal arrests.

To determine a denominator, we looked at various reports that tabulate the number of cyber incidents and cybercrime. The FBI IC3 report for 2016 notes 298,728 complaints received that year.⁵⁷

Based on these numbers, we estimate the enforcement rate at 0.31%. Considering only one in six victims of cybercrime report to law enforcement,⁵⁸ the *effective* enforcement rate estimate may be closer to 0.05%.

Number of Convictions for Internet Fraud



Source: justice.gov

The number of convictions reported by the FBI alone is even lower than the number of arrests used to calculate the cyber enforcement rate. The only DOJ document that Third Way has found that reports prosecution numbers is the FBI Congressional Budget Justification document, which lists them as “Internet Fraud.”⁵⁹ The FBI reports that using the IC3 data to develop law enforcement referrals, it only secured nine convictions in 2016, down from nineteen cases the previous year.⁵⁹

While these cases are important and meaningful in punishing cyber attackers, they represent a very small drop in a very large bucket. And the low enforcement rate for cybercrime has consequences. Cybercriminals are operating with near impunity compared to their real-world counterparts. Given the increasing ease of committing these crimes and the unlikely chance of being caught, it is no wonder that this category of crime is on the rise.⁶⁰

In the face of such a small response from law enforcement, some believe the private sector should take matters into their own hands and go on the offense. A widely-perceived enforcement failure will lead victims to eventually say “enough is enough” and act on their own.

This offensive approach is not to deter attackers but to disrupt their capabilities, including rendering useless their devices, locking accounts, and blocking server access.⁶¹ Proponents of so-called “hacking back” will acknowledge that the impulse comes from a recognition of an enforcement failure and a frustration about the inability to do anything to stop the attacker.⁶² But hack back exposes the counter-hacker to their own liability for unauthorized access to someone else's system and malicious action. Additionally, malicious cyber actors use proxy systems that are tough to identify and retaliations may target systems of innocent individuals. In a well-functioning system, victims have confidence that law enforcement is doing their best to catch the attacker and have a reasonable chance of doing so.

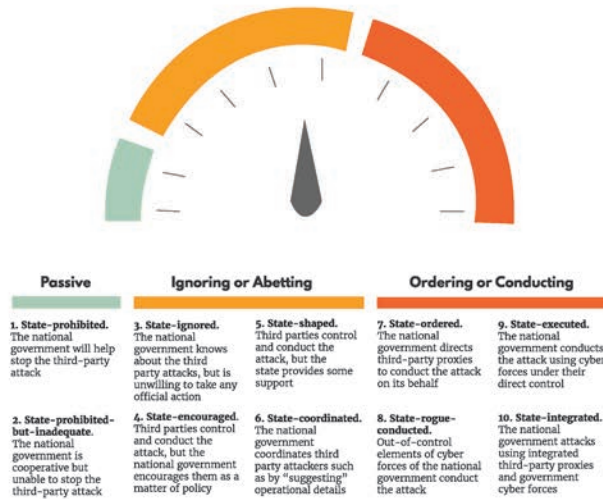
The Cyber Enforcement Gap: Third Way's analysis estimates that the enforcement rate for reported incidents of the IC3 database is 0.3%. Taking into account that cybercrime victims often do not report cases, the effective enforcement rate estimate may be closer to 0.05%.

Furthermore, America's enforcement gap has been largely hidden because there are no good metrics to assess law enforcement response. The number of reported crimes is proportionally miniscule in comparison to the number of actual crimes. Anecdotal data on high profile incidents and prosecutions do not provide a full picture of what's at stake. The traditional crime statistics also do not reflect the kinds of new computer enabled crimes that are happening today.⁶³ And, the lack of clarity in how to report crimes means that state, local, and federal agencies do not report cybercrime in a clear or consistent manner.

There is a clear enforcement gap in cybercrime that must be urgently addressed. The problem is right in front of us, but policymakers are largely not paying any attention to it. The recent indictments against Russian and North Korean state cyber actors may be perceived as progress, but they do not address the large number of crimes that go unnoticed.⁶⁴ The lack of action, the rising costs as a result, and the apparent impunity of these malicious actors would not be tolerated in any other domain. But it often seems like an afterthought in the realm of cyber.

Closing the enforcement gap will also require understanding the motivation of the human attacker and their relationship to foreign states or other non-state actors that might harbor or support them. This is an essential factor in crafting an effective policy solution to compel behavioral change. There are four reactions the state can take toward the attacker: passive, ignore or abet, or order or conduct.⁶⁵ Depending on the nature of the nation state and the cyber attacker(s) and their motivations, the tools used to target a change in behavior of both the state and attackers will vary. It's important to deeply understand the nature of this relationship to employ the most effective solution once the human attacker has been identified.

The Spectrum of State Responsibility



Source: Jason Healey, Atlantic Council

Working with states that prohibit attacks may require increased cooperation or capacity building to be able to coordinate efforts to bring enforcement actions against the attackers. If the state is ignoring or abetting the attacker, diplomatic pressure will need to be brought to bear to change the state's attitude about its complicity in the attacks. This may in some cases bring a different set of more coercive tools to bear. Finally, if the state has direct responsibility for the attacks and is encouraging or conducting them as part of the attacking state's foreign policy, then the victimized nation may have to consider the full spectrum of actions available, beyond law enforcement and diplomacy, against the attacking nations.

Ultimately, if malicious cyber actors are working at the behest of nation-states to advance their objectives through cyberattacks, they are likely to be much more difficult to punish or change their behavior at all. Even if you are able to do so either by sanctioning or arresting them in another country, it is likely that the foreign government sponsor would just recruit others to take up the banner and continue the attacks.

Importantly, although there are a number of nation-states that are using cyberattacks as a tool to advance their objectives, this does not in any way mean the United States can ignore the massive cybercrime wave that is occurring, granting impunity to the large number of malicious cyber actors that may be able to be identified, stopped, and punished. Regardless of whether the behavior is the decision of an individual or the state, whether it's the fingers on the keyboard or the ones signing the order, it is still a human whose decision-making process can be impacted, and who can (and should) feel real consequences.

Rebalancing the US Cyber Approach

Given the magnitude both of the cybercrime wave and the enforcement gap the nation faces, it's clear that the current approach is insufficient. As the number and intensity of cyberattacks has increased, robust efforts at cyber defense are necessary, but not nearly sufficient. A determined attacker will get through even the most heavily defended system. Focusing on making the most secure target possible to the exclusion of a substantial focus on also getting the attacker allows malicious actors to continue to multiply and operate with a sense of impunity. And while there are an infinite number of vulnerabilities and a growing number of attacks, there are a finite number of attackers. To stop those attackers, we must transform both the way we think about cybersecurity and rebalance our efforts to include a greater focus on going after the human attacker.

To be sure, there has been a growing emphasis under the Obama and Trump Administrations in going after malicious cyber actors through law enforcement actions and imposing other types of costs to change their behavior. This includes the number of actions that have been taken against malicious cyber actors working on behalf of adversarial nation-states. However, as the enforcement rate makes clear, these efforts are not nearly enough. Nor have they been sufficiently resourced and given the political leadership necessary to make progress.

We need to change the calculation of malicious cyber actors by balancing defense of systems with an offense designed to stop and deter the human.

Most of the cybersecurity efforts are currently defensive in orientation, focused on protecting systems and networks. Building better firewalls against attacks, creating better passwords, and educating users are all critical. But a strategy primarily developed around building impregnable cyber walls and mistake-proof human users cannot succeed. We need to create a more robust parallel effort around how we identify, stop, and punish the human attacker. We need to change the calculation of malicious cyber actors by balancing defense of systems with an offense designed to stop and deter the human.

It's no surprise that thus far the American government has had a heavy focus on defending systems and networks. This approach has been, in part, driven by a blame-the-victim mentality in cybersecurity. When there is a major cyber breach of a company they are often hauled up before Congress and made to apologize for their lapses, their holes in security, and their failure to have the most up-to-date defenses. To be sure, some of these companies deserve criticism for not taking proper precautions. For example, Equifax, a consumer reporting agency, which holds millions of Americans personally identifiable information, was hacked in 2017

because they failed to update their software after knowing about the risk for months. This led to hackers exploiting the vulnerability, exposing the information of 143 million Americans.⁶⁶ This was preventable and companies that similarly fail to address known vulnerabilities should be held accountable. Corporations in America fear the losses and reputational harm that come from a major breach, and thus focus their efforts on defending their networks and data.

Beyond the private sector, the government's own approach to cybersecurity has also been primarily defensive in nature. In 2008, the Bush Administration adopted a new approach to securing the internet, the Comprehensive National Cybersecurity Initiative (CNCI),⁶⁷ which established a broad series of policies aimed at trying to secure the United States in cyberspace.⁶⁸ Later declassified by President Obama, it was a call to arms establishing and modernizing the government's role in defending networks, sharing information, and increasing cyber-education. The CNCI established the basic parameters of the debate which focused on: network security, securing critical infrastructure, and global supply chain risk mitigation.⁶⁹ This overarching focus on defense is one that has continued in the cybersecurity debate to this day, including the Trump Administration's recently released the *National Cyber Strategy*.⁷⁰ While the Strategy is an important conceptual framework for strengthening law enforcement efforts at home and abroad and imposing consequences on cyberattackers and nation-state sponsors, the Strategy still heavily centers on cyber defense with only a few short sections committed to pursuing hackers. It proposes no advances to how the government will assess its progress on enforcement and has few innovative, new solutions to address the number of tremendous challenges that exist in closing the enforcement gap.

Yet, the government is the only institution with the authority to do anything about the human attacker and the capability to bring them to justice. The government's abilities in this area are quite broad, but in our assessment, priorities and resourcing have been improperly aligned to go after the attacker. When there is a conversation about how the government is going after hackers it is often framed in military terms, which is inapplicable against most of the attackers we see today.

Military leaders have been debating how large a cyberattack must be in order to make it an act of war since the massive Russian denial of service attacks that crippled Estonia in 2007.⁷¹ Those attacks were largely the inspiration for the North Atlantic Treaty Organization's (NATO) efforts to develop the Tallinn Manual, an attempt to set the rules for cyber war.⁷² Multiple efforts have been made to define the rules of cyberwar and to develop Digital Geneva Conventions.⁷³ Given the vast amount of funding the military has to invest in cybersecurity, and the over-militarization of US foreign policy generally, it is no surprise that the debate around when a cyberattack will trigger a kinetic response is robust.

For example, the elevation of US Cyber Command to a unified combat command shows the political consensus in the Executive Branch and in Congress to embrace a military approach. On August 18, 2017, the administration elevated Cyber Command to a unified command, and according to a White House statement, this "... demonstrates our increased resolve against cyberspace threats and will help reassure our allies and partners and deter our adversaries."⁷⁴ This military priority is reflected in Cyber Command's request of approximately \$647 million for fiscal year 2018, a 16% increase over the previous year.⁷⁵ Additionally, in August 2018, the Trump administration relaxed the rules in Presidential Policy Directive 20, which governs the use of US offensive and defensive cyber operations, especially those to "deter foreign election influence and thwart intellectual property theft by meeting such threats with more forceful responses."⁷⁶

Yet, until that threshold is crossed, all of those military cyber-weapons are limited to cyberspace and cannot physically touch the human cyber attacker. While the Pentagon is developing weapons that may deny the attacker access to their tools, these responses may have collateral consequences and are limited in their ability to impose consequences on the individual human attacker. Given the range of types of attacks and attackers, cyber weapons may not be the best response in a particular situation. There are other tools besides military action that can be used to stop the attacker.

Rather than responding with military force, the government can use its Title XVIII authorities to bring law enforcement to bear against the attacker at any time. Unfortunately, the current prioritization undervalues and underinvests in that response. We can only stop this cybercrime wave and close the cyber enforcement gap by transforming law enforcement, enabled by diplomacy, to go after the attacker.

America needs a comprehensive cyber enforcement strategy aimed at identifying, stopping, and punishing cyberattackers, which it currently lacks. This strategy would need both domestic and international components to it as well as the structure and process in place to achieve its objectives. We lay out elements of that strategy below.

Toward a Comprehensive Cyber Enforcement Strategy

In this section we lay out the contours of what a comprehensive cyber enforcement strategy could look like. These broad recommendations are aimed at achieving the fundamental rebalance we aim to see in America's cybersecurity approach to dramatically improve the country's security. Over a multi-year initiative, Third Way will develop more detailed policy proposals to advance these efforts.

Below we detail our recommendations for areas of priority that require urgent attention by policymakers. Some of these recommendations are aimed at building upon existing streams of efforts while others propose new reforms. These recommendations fall into three general categories of those that deal with: 1) domestic enforcement reform, 2) international coordination and cooperation reform, and 3) internal US government reform efforts to put in place the structure and process to lead all of these efforts.

Domestic enforcement reform

Recommendation #1: A Larger Role for Law Enforcement

Absent a state of war, the primary US government agencies with the authority and ability to identify, stop, and punish the humans responsible for these attacks are law enforcement—enabled by our diplomats and allies. Law enforcement is how we deal with people who have broken our laws in peacetime. Recent high-profile enforcement actions demonstrate what is possible when law enforcement and diplomats target individual attackers and point to a new way forward.

For example, in 2015, after a series of cyber espionage attacks on intellectual property in the US private sector, the Obama administration exerted diplomatic pressure on China. Under

the threat of sanctions, the Chinese government arrested individuals accused of commercial cyberespionage.⁷⁷ Experts believe the individuals arrested to have ties to the cyber offense unit of the People's Liberation Army (PLA).⁷⁸

The US Government was able to investigate and indict twelve Russian GRU (Main Intelligence Directorate, abbreviated GRU) agents for hacking the Democratic National Committee and the Clinton Campaign during the 2016 election. The indictment detailed the methods and technologies used by the GRU to execute the hack. The investigators were also able to obtain the names of individuals responsible for executing, coordinating, and ordering the hack.⁷⁹ Even against the most sophisticated nation-state actors it is possible to identify and bring indictments against the individuals who launch the attacks.

In cyber policy circles, there are many who have argued that enforcement actions cannot have an impact when it comes to America's adversaries who use cyberattacks to target our country. But enforcement actions taken against malicious cyber actors even in the most difficult cases can still have a substantial impact. Deputy Attorney General Rod Rosenstein recently laid out the Department of Justice's view on this very issue, arguing that indictments and prosecutions are an important tool in these cases for a number of reasons, including: 1) the defendants may one day face a trial if there is a change in their government's calculus or they travel to another nation that cooperates with the United States in these efforts; 2) public indictments can provide some level of deterrence by raising the risk that these individuals will be held accountable, making them less attractive for future attacks; 3) these actions demonstrate the ability of US law enforcement to attribute attacks and charge hackers, which may deter others; 4) federal indictments in the US criminal justice system given its evidentiary standards are often taken seriously by other countries, which could impact their relationship with the offending countries; and 5) victims deserve justice for the attacks that were perpetrated against them.⁸⁰

But it's not enough to just bring indictments leaving the hackers on the loose in foreign lands. The ultimate goal is to take them off the field completely, and law enforcement, enabled by diplomats, does that too.

It's time to rebalance cyber resources, beefing up the capacity of law enforcement and diplomats to focus on bringing to justice those people who are stealing Americans' hard-earned money, ideas, and personal data for nefarious purposes.

Unfortunately, American law enforcement and diplomatic efforts are severely under-resourced to address the growing cyber-crime wave. In fiscal year 2017, the Department of Defense spent \$7.2 billion on cybersecurity broadly, nearly ten times the cybersecurity resources of the Department of Justice.⁸¹

As the recent CSIS report highlighted, America needs better cyber forensic capabilities and training.⁸² These resources must be committed to:

- **Forensics Training for Law Enforcement:** In 2018, the National Computer Forensic Institute (the nation's only federally-funded training center dedicated to instructing state and local law enforcement officers, prosecutors, and judges in digital/cybercrime investigations) was only provided \$18.9 million for its training efforts.⁸³ This 2018 funding level is only enough to train approximately 1,200

students even though the Institute has the capacity to train over 3,000 students annually if fully funded.⁸⁴ Yet some law enforcement officials are receiving just 12 hours of digital evidence training a year.⁸⁵

- **Technical Assistance for Local Law Enforcement:** Even in the best of circumstances, not every officer in the country will be able to become an expert on digital evidence collection, so better forensic capabilities will require technical help for local law enforcement. For example, the New York County District Attorney's office only has 15 forensic specialists on staff to support 550 prosecutors handling over 100,000 cases annually.⁸⁶ State and local law enforcement rarely have the same level of technology available as the federal government. The costs of running a cybercrime division are simply too high for many local offices. New York City built a digital forensic lab in 2016 that cost \$10 million—a price tag well beyond what most cities can spend.⁸⁷
- **Improve Crime Labs:** Just 79 of the 409 publicly funded crime labs in the United States offered dedicated digital evidence support services according to a DOJ report.⁸⁸

Without these resources, law enforcement officials cannot confront the new challenges posed by the cyber domain. In particular, digital evidence collection is a core component of most cyber investigations, yet federal, state, and local law enforcement have been hampered by their lack of training on such evidence collection and a lack of expert personnel that can be called upon to provide technical assistance in cyber investigations.⁸⁹

It is time to rebalance these resources, beefing up the capacity of law enforcement and diplomats to focus on bringing to justice those people who are stealing Americans' hard-earned money, ideas, and personal data for nefarious purposes.

Recommendation #2: A Cyber Enforcement Cadre

In order to transform the government's enforcement efforts, we must be willing to address not only cybersecurity workforce shortages, but the way that workforce is trained, incentivized, and retained to hunt and catch cybercriminals.

There are 299,000 unfilled cybersecurity positions in the United States and the gap is expected to reach 1.8 million by 2022, according to a 2018 report authored jointly by the Department of Commerce and DHS.⁹⁰ The gap in unfilled cybersecurity positions covers both the private and public sector and vacancies range from information technology (IT) specialists to law enforcement cyber investigators. The large vacancy in positions affects the government and companies' ability to improve their cybersecurity and law enforcement's ability to go after cybercriminals. There is also a severe lack of diversity in this workforce, which could vastly improve the effectiveness of the workforce as a whole.⁹¹

The ways that law enforcement personnel are trained to be able to handle digital forensics of these crimes will need broad transformation.

One of the central issues the US government is confronting is recruiting capable cyber talent and this has had a direct impact on US enforcement agencies. A 2015 Department of Justice

Office of the Inspector General (OIG) report highlighted a need to increase pay for cybersecurity professionals, particularly those that serve in cyber investigation roles working within the National Cyber Investigation Joint Task Force, a multi-agency cyber coordinating entity within the federal government.⁹² Additionally, the report notes challenges with the lengthy security clearance process, prohibiting the use of marijuana in the past 3 years, and prohibiting illegal drug use in the past 10 years, posing a challenge in recruiting a younger generation used to a more permissive environment.⁹³ Once recruited, there are challenges in retention and promotion that must be addressed. The recent departure of four senior FBI cyber officials on top of an additional 20 FBI cybersecurity officials in the past five years for high-paying corporate positions that can exceed \$300,000 highlights the challenges of retaining senior talent in the face of lucrative private sector positions.⁹⁴

There are also challenges with ensuring that law enforcement is properly trained to conduct cyber investigations. Preparing law enforcement personnel to handle cybersecurity cases will require increasing the technical capability of multiple specialties: detectives who investigate crime, specialized forensic technicians who analyze digital devices and signatures, and first responders who secure crime scenes.⁹⁵ A recent report by the Center for Strategic and International Studies (CSIS) surveyed law enforcement personnel and discovered that many don't know how to make basic requests to technology companies for data that they need to investigate crimes in general, not just computer-enabled crimes.⁹⁶ The ways that law enforcement personnel are trained to be able to handle digital forensics of these crimes will need broad transformation.

Recommendation #3: Better Attribution Efforts

Attribution, or identifying the origin and individuals responsible for a cyberattack, is difficult and time consuming, but not impossible.

It often requires teams of investigators comprised of forensic experts, law enforcement officials, and cybersecurity professionals.⁹⁷ Technologies like VPNs, the Tor network, and advanced encryption used by malicious cyber actors add to the difficulty by masking identifying information. Tools created using machine learning allow malicious actors to perform reconnaissance, or information-gathering efforts, efficiently and to a much higher degree of accuracy.⁹⁸ The solutions offered by law enforcement often raise serious civil liberties concerns and the issue remains a challenge for local, state, and federal officials, and the private sector—as was apparent in the Apple-FBI dispute regarding the San Bernardino case in 2016.⁹⁹

Attribution often requires close cooperation between law enforcement and other government entities and victims of cyberattacks for evidence collection and sharing of threat intelligence. Law enforcement is unable to pursue cases against cybercriminals if victims of cyberattacks do not report these attacks and share evidence with the proper authorities. Intelligence agencies are also unable to collect and analyze cyber-threat intelligence if there is not an effective mechanism in place for information sharing from the private sector and government entities. While law enforcement and intelligence agencies do and should face restrictions on accessing data for attribution without due process, it is worth assessing whether the current systems and processes in place allow for the most effective and efficient sharing of cybercrime information between victims, particularly in the private sector, and government enforcement entities.

Because of a lack of physical evidence, cyber attribution has to deal in degrees of certainty rather than absolutes.¹⁰⁰ Most attribution reports from cybersecurity organizations will refrain from

making an outright accusation. Instead, they use subjective levels such as low, medium, or high confidence.¹⁰¹ Translating this into evidence that a prosecutor could present in court in front of judge and jury can be an onerous task.¹⁰²

However, considerable progress has been made on attribution in cyber investigations. The indictments against nation-state actors like China's PLA and Russia's GRU show that attribution is possible against even the most sophisticated actors.¹⁰³ The change in the attitude of cybersecurity experts to the US government attribution of the Sony attack to North Korea shows the evolution of attribution mechanisms in the last few years.¹⁰⁴

Attribution made by or against a nation-state may require human sources or information obtained through technologies the victim government does not wish to reveal. In the investigation into Russian hacking during the 2016 presidential election, many individuals were critical of the initial DHS report for not containing enough information and were suspicious of the attribution made to Russia.¹⁰⁵ After the government disclosed more information regarding the hack and other offensive operations, most analysts and experts accepted that Russian actors hacked the Democratic National Committee (DNC).¹⁰⁶

Further, given the international nature of many of these crimes, attribution by the United States will also have to be sufficiently credible to convince foreign partners to take action. Rising distrust of the United States in the global space, especially in areas related to intelligence, have heightened the need to be able to provide transparent and credible attribution for cyberattackers. Attributing attacks is the first stage in a process that allows for enforcement actions to be taken against malicious cyber actors, whether that be law enforcement action or sanctions. US diplomatic officials have taken a leading role in building up coalitions of countries that can coordinate on attribution issues, providing determinations on who perpetrated an attack that have more diplomatic might on the global stage than the United States standing alone.¹⁰⁷

Progress has been made in this direction with US attribution efforts having been closely coordinated with partner nations on some recent cases. For example, this month, officials from the United States, United Kingdom, and the Netherlands released coordinated announcements attributing the targeting of the Organization for the Prevention of Chemical Weapon to the GRU.¹⁰⁸

The Trump Administration's newly proposed Cyber Deterrence Initiative is a potential avenue for such a coalition.¹⁰⁹ But to ensure this Initiative is most effective, it must also address the issues that have impeded joint attribution in the past, including significant delays caused by bureaucratic processes and challenges in information sharing between the United States and partner countries. These joint attribution efforts will involve more than just collecting, analyzing, and sharing digital evidence. In the end, the decision by governments to publicly identify malicious cyber actors, particularly nation-state actors, will be a political decision by their leaders. If all of these international efforts are to be effective and coordinated, the State Department needs a senior-level person resourced and empowered to ensure that our diplomatic efforts are consistent with the goal of increasing our ability to identify, stop, and punish the attacker.

All of these challenges can begin to be met or at least mitigated by:

- More resources for technological advances in cyber investigations dedicated to enhancing cyber attribution efforts at federal and state levels. Systems and processes for cyber attribution are currently in their infancy when compared

to physical crime and often they are too costly for many states and localities to pursue on their own.

- The federal government advising system operators of the tools and best procedures to use when breached so they can gain the maximum forensic evidence.
- Building alliances, substantially improving information sharing processes and mechanisms between partner nations, and streamlining bureaucratic processes to improve the timeliness and impact of joint attribution efforts.

Recommendation #4: A Carrot and Stick Approach to Fugitives

In some cases, the criminals may be difficult to find or hiding in countries that provide them safe haven. The United States need not give up just because a criminal is beyond the arm of the law. It can reinvigorate enforcement tools used to impose consequences on cyber fugitives— both in offering rewards for their apprehension or imposing sanctions while they're at large.

A comprehensive strategy to deter and apprehend cybercriminals requires the use of a "carrot and stick" approach. The "carrot" could be the use of a reward-based system to incentivize the sharing of information that can lead to an arrest of malicious cyber actors. The "stick" is the use of targeted sanctions on cybercriminals and their possible nation-state or organizational sponsors.

The United States can reinvigorate enforcement tools used to impose consequences on cyber fugitives—both in offering rewards for their apprehension or imposing sanctions while they're at large.

Current "Most Wanted" programs can be expanded to incentivize the capture of cybercriminals. The FBI currently maintains what is known as the "Cyber's Most Wanted" list to raise public attention on cyber-fugitives and it should be evaluated if the use of rewards to incentivize information on cybercriminals can be expanded even further. As of September 2018, this list includes 42 malicious cyber actors from many different countries but additional individuals have been listed and then delisted once they have been captured.¹³⁰ The FBI also maintains a most wanted list for criminals involved in others types of crimes. The most well-known use of a criminals list is the FBI's "Ten Most Wanted Fugitives" list. The FBI has used a "Ten Most Wanted Fugitives" list for various crimes since the 1950s, and over the years over 519 fugitives have been on the list with the majority eventually being apprehended.¹³¹ According to the FBI, "one hundred and sixty-two of the 'Ten Most Wanted Fugitive' apprehensions have been the result of citizen recognition of 'Ten Most Wanted Fugitive' publicity."¹³² The lists are designed to help law enforcement garner public attention to apprehend criminals who otherwise might not receive attention and often tie rewards that are offered to the reporting of information that leads to arrest or apprehension.¹³³ The FBI in the past has applied the same incentive-based reporting approach to the "Cyber's Most Wanted" list with rewards for certain criminals being as high as \$100,000.¹³⁴ However, there are currently very few cybercriminals listed that are tied to a reward. The rewards-based system for information on certain crimes has been an important tool in apprehending criminals and policymakers must evaluate whether incentives for information on cybercriminals can be expanded even further.

As we expand the use of incentives, we can also use punitive tools to impose consequences on cyber fugitives. Where the foreign nation is unwilling or unable to assist the United States in the prosecution of a cybercriminal, individual sanctions can be used by the US government to punish individuals responsible for malicious cyber-enabled activities who remain outside of the United States. The Department of Treasury can impose economic and financial sanctions. These may include such things as asset freezes and travel bans on individuals. The United States has many existing sanctions regimes, but the use of sanctions for cyber enforcement is a relatively recent development.¹¹⁵

The Department of Treasury Office of Foreign Asset Control's (OFAC) cyber-related sanctions program was instituted in April 2015 with President Obama's Executive Order 13694 to block the property and interests in property of persons who are responsible or complicit in malicious cyber-enabled activities.¹¹⁶ These sanctions were expanded by President Obama in December 2016 and now allow for the sanctioning of individuals or entities whose activities either directly or indirectly present a "significant threat to the national security, foreign policy, or economic health or financial stability of the United States."¹¹⁷

Sanctions can also be issued against persons or organizations when we suspect a link to a nation-state sponsor. For example, the United States has a specific set of sanctions targeting cyber-enabled malicious activity and nation-state sanctions regimes such as those placed on North Korea and Iran.¹¹⁸ In addition, the "Countering America's Adversaries Through Sanctions Act" was enacted in 2017 to authorize sanctions against any person who engaged in malicious cyber activity against a person or democratic institution on behalf of the Russian government.¹¹⁹

Key partner nations and multilateral organizations like the European Union and the United Nations have sanctions regimes that can be equally, or in some cases more, effective in punishing hard to reach malicious cyber actors and their nation-state sponsors.¹²⁰

By revisiting a carrot and stick approach to apprehending cyber-fugitives as part of an overarching strategy, US enforcement agencies can begin to impose consequences even when the perpetrator is at large.

International cooperation and coordination reform

Recommendation #5: Ambassador-level Cyber Quarterback

Not only must law enforcement transform itself domestically, but it must also transform the ways it works across international borders. Since the early days of the internet, attempts to identify hackers have faced bureaucratic hurdles caused by the multiple jurisdictions involved, the most complex of which require international cooperation.¹²¹ For many law enforcement agencies, the difficulties of getting international cooperation to trace or arrest a malicious actor are extremely daunting.¹²²

The global nature of the cyber threat requires dedicated and deliberate leadership and coordination at the highest echelons of the US government to enhance international coordination and cooperation on closing the enforcement gap. Given the scope of countries that are impacted in a cybercrime investigation, little progress can be made in these efforts if America's cyber diplomacy and development efforts are not expanded and diplomatic ties to partner nations around the globe are not strengthened. To catch international cybercriminals, we'll need a

coordinated international effort, cooperation on building the case, and cooperation on bringing the criminals into custody.

Effective engagement with other countries on cyber threats requires a coordinated international effort as we make catching cybercriminals a top priority for the United States. To have an effective offense, we need a strong quarterback. Unfortunately, the State Department's cyber coordinator being downgraded under the Trump Administration leaves US international efforts without a leader.¹⁵³

Effective engagement with other countries on cyber threats requires a coordinated international effort as we make catching cybercriminals a top priority for the United States. To have an effective offense, we need a strong quarterback.

Congressional efforts to raise the level of the State Department's Coordinator for Cyber Issues to a Senate-confirmed ambassador position are an important step in ensuring the United States has the leadership it needs to strengthen international cooperation and coordination.¹⁵⁴ The Office of the Coordinator for Cyber Issues has played an important role in enhancing the vital operational-level cooperation that occurs between US law enforcement and federal agencies, including the Departments of Homeland Security and Defense, and their foreign counterparts. But a Congressional authorization to elevate the Office of the Coordinator for Cyber Issues is not enough. The Office must also be provided with a clear mandate to include a focus on closing the enforcement gap in its work, including strengthening its efforts on attribution and diplomatic training programs, and the necessary resources and personnel by Congress to be able to do so. This is critical to drive forward a rebalance in America's cybersecurity approach to one that puts the State Department front and center as a key entity for progress.

America's diplomats are key to making a dent in international cybercrime and changing the malicious cyber behavior of nation states and non-state actors more broadly. To make progress, the United States cannot go at these missions alone. It must build a posse of like-minded countries that will complement and enhance our efforts. This means that strengthened international cooperation and alliance building to collectively respond to shared cyber threats, including those posed by nation states, must be a top priority for the US government. The United States must also work to strengthen its leadership in international organizations that deal with these issues, such as the UN, the Group of Seven (G7), NATO, and others, to play a leading role in decision-making and not work to weaken and attack these alliances as President Trump has done on a number of occasions.¹⁵⁵

Recommendation #6: Stronger Tools in the Diplomacy Arsenal

To catch cybercriminals, we'll need international assistance in building the evidence against them. Bilateral agreements facilitate cooperation between the United States and other governments in cybercrime investigations.

Mutual legal assistance treaties (MLATs) and mutual legal assistance agreements (MLAAs) are one such tool to facilitate cooperation on cyber-enabled crime investigations and prosecutions. These binding treaties and agreements are typically bilaterally signed between the United States and other countries to formalize the parameters of their criminal justice cooperation.¹⁵⁶ These treaties can be critical tools for sharing data and digital evidence in cyber investigations

and prosecutions.¹²⁷ Right now the process under these agreements can be very lengthy and administratively burdensome. Congress has taken some action to try to help make this process more efficient. For example, they have worked to facilitate cross-border data sharing directly between US technology companies and foreign governments.¹²⁸ The recently enacted “CLOUD Act” allows the United States to enter into agreements with other countries to provide direct access to data held by technology companies while also raising the standards of civil liberties.¹²⁹ Congress must continue to perform its oversight function in evaluating the effectiveness of any “CLOUD Act” agreements and assessing whether any further legislative changes to these legal assistance processes are needed.

Treaties can be critical tools for sharing data and digital evidence in cyber investigations and prosecutions.

Once the United States has ultimately built cases against these cybercriminals, it will need help bringing them into custody. Once they have an arrest warrant, American authorities can ask INTERPOL, the global police cooperation body, to issue a Red Notice, which asks foreign authorities to locate and provisionally arrest an individual pending their extradition.¹³⁰ Once a Red Notice is issued for a cybercriminal, these persons are placed on lookout lists and, if they come to the attention of police in other countries the United States can request that they be provisionally arrested or file a request for extradition.¹³¹ Extradition treaties allow US authorities to ask other countries to hand over an individual for prosecution or to serve a sentence following a conviction in American courts. The United States has signed extradition treaties with over 100 countries.¹³²

Additionally, the United States should continue to utilize the Council of Europe’s 2001 Convention on Cybercrime (also known as the Budapest Convention) to facilitate cooperation on cybercrime. This treaty was the first binding international treaty that sets common standards on investigations and criminal justice cooperation on cybercrime and electronic evidence. It remains the most wide-reaching cybercrime treaty there is and has now been ratified or acceded by the United States and 60 other countries.¹³³ Expanding the number of countries that ratify or accede to the Budapest Convention is critical to ensure it can have far-reaching impact because it can be a diplomatic tool to push member countries to uphold their obligations. However, if this treaty is to be most effective, it must not just be adopted by like-minded countries. This will require sustained US leadership in pushing countries who have previously opposed its provisions to come on board. Yet, even in countries that have ratified or acceded to the Convention, changes in national laws to comply with the treaty obligations and capacity building for criminal justice actors in the standards of the Convention remain big gaps in certain nations that need to be addressed. As one of the only binding agreements that exists globally on cybercrime, America’s diplomats can work to expand the number of countries that ratify this treaty.

Underneath the frameworks established by international agreements, American authorities are able to take advantage of multilateral tools that exist to try to locate these actors overseas in specific cases and either prosecute them in the United States or the country they are apprehended in. However, these initiatives require resources, personnel, and political leadership from the United States to remain effective.

Recommendation #7: Better International Capacity for Enforcement

US law enforcement has a long way to go to make a dent in the cybercrime wave. But many other nations require far greater capacity building to be able to complement these US efforts.¹³⁴

To strengthen the capability of partner nations, the US government must assess and expand its support to global cyber enforcement capacity building. It must help foreign authorities understand and address the threat as it transforms itself. Currently, the United States provides capacity building assistance on cybersecurity and cybercrime to countries through US diplomatic, development, and international judicial programs.¹³⁵ US enforcement agencies also have personnel and agents posted in key countries who help facilitate cooperation and support capacity-building efforts on cybersecurity and cybercrime.¹³⁶

It is clear that the current levels of funding and manning for capacity building efforts are not adequate to meet the challenge. As the Trump Administration has continued to deprioritize America's diplomatic and development efforts, requesting to gut funding to critical global initiatives¹³⁷ and decimating the workforce,¹³⁸ Congress must push back and ensure adequate, and in some cases expanded, funding is provided to bilateral and multilateral cyber capacity building efforts. The United States cannot say it prioritizes cybercrime capacity building, as the new *National Cyber Strategy* proclaims, without ensuring the resources are provided to support this.¹³⁹

However, the United States does not have to go at this capacity-building alone. There are capacity-building efforts being undertaken for criminal justice actors around the globe, many supported by the United States, by entities like the United Nations,¹⁴⁰ INTERPOL,¹⁴¹ the Organization for Security and Co-operation in Europe,¹⁴² and others in the private sector.

Capacity-building efforts are also an opportunity to strengthen international support for rule of law, privacy, civil liberties, and human rights.

These capacity-building efforts are also an opportunity to strengthen international support for rule of law, privacy, civil liberties, and human rights. As governments around the globe have strengthened their cybersecurity laws, these laws and strengthened cyber capabilities have been used as a tool in certain countries to crackdown on dissidents, opposition figures, and activists.¹⁴³ These laws may help to strengthen efforts to go after cyberattackers but, if used for nefarious reasons, they can be powerful tools to stifle dissent and restrict powerful forces needed for democratization and social change.¹⁴⁴ As the United States works to strengthen its international cooperation on cyber enforcement, this work must match with calls to respect privacy, civil liberties and human rights, and criticism for actions that do not do so.

Structural and process reform

Recommendation #8: Better Success Metrics

To begin to make improvements in the government's ability to bring enforcement actions against cybercriminals, there must be a comprehensive assessment of current government efforts across all agencies with a role in cyber enforcement to determine what is working, what might need to be amplified, and what might need to change. At a minimum, without baseline statistics it is difficult to measure government efforts, develop budget estimates for current levels of effort, and

make an informed case for budget increases necessary to support increased enforcement levels. This baseline does not currently exist.

It's difficult for outside researchers to assess the level of enforcement activity taken by the US government, as we discovered. But even the government's own analysis indicates there's no reliable measurement of the problem. In July 2016, the Department of Justice's Inspector General found that the process that the FBI uses to prioritize cyber threats was subjective and open to interpretation, and that the Bureau lacked a system that would allow it to determine whether cyber threats were appropriately prioritized.¹⁴⁵ Without accurate data on cybercrime, law enforcement cannot make reasoned policy decisions to best deal with the issue.¹⁴⁶ The Uniform Federal Crime Reporting Act of 1988 requires all federal agencies to report federal crime offenses to the FBI, yet there are agencies that have never reported crime data to the FBI.¹⁴⁷ The National Academies of Science has recommended a data collection framework modeled off of one utilized by United Nations entities that would provide reliable and comparative data on crime beyond what is currently available.¹⁴⁸ Better reporting measures would also assist in lowering the number of unreported crimes.¹⁴⁹

Without accurate data on cybercrime, law enforcement cannot make reasoned policy decisions to best deal with the issue.

In addition to the lack of a process to determine prioritization of the cyber threat, the FBI lacks comprehensive performance metrics that set case targets for cyber fraud, a large and growing category of criminal activity.¹⁵⁰ The lack of comprehensive performance metrics stands in stark contrast to the targets set for white collar crime, mortgage fraud, and criminal enterprises and gangs.¹⁵¹

A baseline assessment on the government's cyber enforcement efforts will allow for the eventual setting of targets for agency performance on a number of different metrics. For example, the US Secret Service (USSS) sets targets for each year, reported to Congress, on a number of cyber-related measures. This includes the amount of dollar-loss prevented by Secret Service cyber investigations as well as the number of law enforcement officials trained in cybercrime and cyber forensics. In fiscal year 2017 alone, the USSS set a target to prevent \$600 million in the public financial loss that was prevented due to the agency's cyber investigations. It far exceeded that target.¹⁵² However, these targets do not appear to include targets set for arrests and prosecutions and nor do the targets set by other enforcement agencies.¹⁵³ Assessing the government's efforts now on cyber enforcement will allow for the setting of targets on enforcement actions taken moving forward.

Recommendation #9: Organizational Changes and Interagency Cooperation

Cybercrime remains pervasive and the US government's enforcement efforts to counter this threat must be made as efficient and effective as possible. This must include necessary reforms to de-conflict the often overlapping mandates of the numerous US government agencies involved in enforcement. The many federal agencies with special agents that all have a role in cyber investigations and the number of state and local law enforcement agencies also leading investigations has led to similar or overlapping responsibilities between these entities. At the federal level in particular, this can lead to inefficiencies, redundancies, and difficulties in

ensuring congressional oversight efforts are tied to an overarching strategic cyber enforcement approach across agencies.¹⁵⁴

Efforts have been undertaken already to enhance coordination between these various agencies. For example, the National Cyber Investigative Joint Task Force (NCIJTF) was established in 2008 to serve as focal point for government coordination and information sharing on cyber investigations. The FBI-led NCIJTF serves as the national focal point for coordinating cyber threat investigations and allows for information sharing across over 20 member agency representatives from law enforcement, the intelligence community, and the military.¹⁵⁵ FBI also leads state and local task forces out of its field offices to coordinate domestic cyber threat investigations at the state and local level.¹⁵⁶ In addition, the USSS coordinates a network of Electronic Crimes Task Forces to strengthen its efforts to prevent, detect, and investigate various types of electronic crimes.¹⁵⁷

However, even with the creation of these task forces, there's continued confusion on which agency has the lead to investigate certain types of cybercrime. A 2015 congressional report found that the similar or overlapping missions of enforcement agencies has continued to cause confusion on which agency has the lead on investigating certain crimes, particularly when multiple agencies are involved in an investigation. This also creates confusion among the American people on what agency they should even report to if they become victim of a cybercrime.¹⁵⁸

Reforms need to focus on de-conflicting the missions of the agencies responsible for cyber enforcement, focusing on streamlining efforts, reducing duplication, and clarifying jurisdiction. Without these reforms, issues will remain on how to accurately assess the progress of each of these agencies and link that progress to an overarching strategic approach tied to resources and personnel. To ensure these investigations are as efficient and effective as possible, investigators working on complicated and multi-jurisdictional cybercrimes need clarity on which agency is taking the lead on coordinating the effort.

Recommendation #10: Centralized Strategic Planning

All of these areas of focus must be supported by an overarching, comprehensive strategy for US cyber enforcement aimed at identifying, stopping, and punishing global cyberattackers. That overarching strategy must include a plan to transform the interagency cooperation on cyber enforcement, both domestically and internationally. No single agency can tackle this behemoth of a challenge alone. A comprehensive domestic strategy would require unparalleled cooperation between the myriad federal agencies that have a role in cyber investigations.

A recent assessment by the non-partisan Government Accountability Office (GAO) underscores that the government still lacks a comprehensive cybersecurity strategy that allows for effective oversight.¹⁵⁹

And the Trump Administration's recently released *National Cyber Strategy* does not meet the benchmarks for an effective strategic approach that allows for proper oversight.¹⁶⁰ This document does contain priorities for strengthening cyber enforcement and is an important first step. However, there remains little detail, at least publicly available, as to how federal, state, and local agencies plan to implement it. This document echoes some of the concerns expressed by the 9/11 Commission in its critical assessment of the US counterterrorism strategic approach before these catastrophic terrorist attacks.¹⁶¹ The Commission noted that while the US government cannot promise that a terrorist attack will never happen on American soil again "the American people

are entitled to expect that officials will have realistic objectives, clear guidance, and effective organization. They are entitled to see standards for performance so they can judge, with the help of their elected representatives, whether objectives are being met.¹⁶³ In order to achieve the necessary transformation, we will have to develop these standards and benchmarks.

The US government needs a position to oversee and coordinate a national cyber strategy to ensure that there is proper attention and resources dedicated for this pervasive national crisis, benchmarks for progress are tracked and evaluated, and there is clarity in mission of different agencies to avoid duplication.

A strategy will be most effective when there is White House leadership managing and coordinating a whole-of-government response. When the country has faced tremendous threats in the past, “czar” positions were created within the executive branch to mobilize and coordinate resources, streamline processes, and work to coordinate the efforts of the numerous government agencies involved.¹⁶³ Most recently, the Obama Administration created the position of Ebola response coordinator, known as the Ebola Czar, to coordinate the federal government’s ability to combat Ebola.¹⁶⁴ Similarly, the US government needs a position to oversee and coordinate a national cyber strategy to ensure that there is proper attention and resources dedicated for this pervasive national crisis, benchmarks for progress are tracked and evaluated, and there is clarity in mission of different agencies to avoid duplication.

The Trump administration has taken the opposite approach. The Trump White House has actually scaled back cybersecurity coordination not strengthened it,¹⁶⁵ eliminating the White House Cyber Coordinator position within the National Security Council (NSC) and leaving coordination to two senior director-level NSC officials.¹⁶⁶ NSC officials often operate with little resources and support personnel. In comparison, the operating budget of the Office for National Drug Control Policy, the office of the Drug Czar, in fiscal year 2018 alone was \$18.4 million for operating costs,¹⁶⁷ which has been even higher in years past.¹⁶⁸ The country is facing a national cybersecurity crisis and there is no senior official empowered with the resources to coordinate a comprehensive cyber strategy that includes a significant focus on closing the cyber enforcement gap.

What are the federal agencies involved in cyber enforcement?

Many federal agencies have a role in cyber investigations, including the FBI, the Secret Service (USSS), the Immigration and Customs Enforcement’s Homeland Security Investigations (HSI), and others.¹⁶⁹ State and local law enforcement agencies also lead on many cybercrime investigations. While each of these agencies has a vital role in cyber enforcement, there are also some similar or overlapping responsibilities between them. At the federal level in particular, this can lead to inefficiencies, redundancies, and difficulties in ensuring congressional oversight efforts are tied to an overarching strategic cyber enforcement approach across agencies.¹⁷⁰

The descriptions provided by the Secret Service, Homeland Security Investigations, and the FBI concerning the scope of their mandate on cybercrime demonstrates the lack of clarity in their investigation jurisdictions:

USSS: “Cybercrime, including computer intrusions or attacks, transmissions of malicious code, password trafficking, or theft of payment card or other financial payment information.”¹⁷¹

HSI: “Cyber-based domestic or international cross-border crime, including child exploitation, money laundering, smuggling, and violations of intellectual property rights.”¹⁷²

FBI: “Cybercrime, including computer intrusions or attacks, fraud, intellectual property theft, identity theft, theft of trade secrets, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity.”¹⁷³

Conclusion

Before 9/11 the US government lacked a strategic approach to the threat of terrorism. While the 9/11 Commission documented enormous efforts that were undertaken by the US government to detect and disrupt the terrorist threat, it also found tremendous barriers to progress, including a lack of prioritization of the threat, competing priorities and immense bureaucratic challenges.¹⁷⁴ Some of the challenges they found also stymie a strategic approach to cybersecurity. They noted that a comprehensive approach to counterterrorism was limited by: law enforcement priorities guided by local FBI field offices as opposed to by an overarching national approach;¹⁷⁵ a lack of a significant shift in resources at the FBI to meet the threat;¹⁷⁶ insufficient training for law enforcement;¹⁷⁷ the minimization of the important diplomatic role of the State Department;¹⁷⁸ and the failure of Congress to adjust itself to address the rise of the transnational terrorism threat and conduct proper oversight.¹⁷⁹ The state of the US government's cybersecurity efforts today draw alarming parallels to these pre-9/11 challenges.

To transform the US government's ability to improve its ability to identify, stop, and punish the attacker, we will need a strategy that doesn't just focus on building a better safe, but focuses on catching the safe-cracker.

We have enough examples of successful prosecutions to know that while finding and punishing the attacker is hard, it's not impossible. Today, we lay the cornerstone of that foundation, and dedicate ourselves to building a more complete cyber enforcement architecture.

ENDNOTES

- 1 Chuang, Tamara. "Pay Us Bitcoin or Never See Your Files Again: Inside the Highly Profitable Underworld of Ransomware." The Denver Post, The Denver Post, 8 Mar. 2018, www.denverpost.com/2018/03/04/computer-ransomware/. Accessed 19 Oct. 2018.
- 2 Chuang, Tamara, and David Migoya. "SamSam Virus Demands Bitcoin from CDOT, State Shuts down 2,000 Computers." The Denver Post, The Denver Post, 22 Feb. 2018, www.denverpost.com/2018/02/21/samsam-virus-ransomware-cdot/. Accessed 19 Oct. 2018.
- 3 Colorado Department of Transportation. "CDOT Cyber Incident After-Action Report." 17 July 17, 2018, pp 3. <https://www.colorado.gov/pacific/dhsem/atom/129636>. Accessed 3 Oct. 2018.
- 4 Chuang, Tamara. "Ransomware Strikes CDOT for Second Time Even as Agency Still Recovering from First SamSam Attack." The Denver Post, The Denver Post, 2 Mar. 2018, www.denverpost.com/2018/03/01/cdot-samsam-ransomware-attack/. Accessed 19 Oct. 2018.
- 5 Kearney, Laila. "Atlanta Officials Reveal Worsening Effects of Cyber Attack." Reuters, Thomson Reuters, 6 June 2018, www.reuters.com/article/us-usa-cyber-atlanta-budget/atlanta-officials-reveal-worsening-effects-of-cyber-attack-idUSKCN1231M. Accessed 19 Oct. 2018.
- 6 Quinn, Samm. "Hospital Pays \$55,000 Ransom; No Patient Data Stolen." Daily Reporter, Daily Reporter, 16 Jan. 2018, www.greenfieldreporter.com/2018/01/16/01162018dr_hancock_health_pays_ransom/. Accessed 19 Oct. 2018.
- 7 Sophos. "SamSam : The (Almost) Six Million Dollar Ransomware." 19 July 2018, pp. 8. <https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf>. Accessed 19 Oct. 2018.
- 8 Deere, Stephen. "CONFIDENTIAL REPORT: Atlanta's Cyber Attack Could Cost Taxpayers \$17 Million." Ajc, The Atlanta Journal-Constitution, 2 Aug. 2018, www.ajc.com/news/confidential-report-atlanta-cyber-attack-could-hit-million/GAljmmndAF3EQdVWIMcXS0K/. Accessed 19 Oct. 2018.
- 9 This number includes 2016 incidents that involved a systemic or targeted breach of a system and does not include privacy crimes, online harassment, or crimes against children. See: Federal Bureau of Investigation. "2016 Internet Crime Report." 22 June 2017, pp. 17. https://pdf.ic3.gov/2016_IC3Report.pdf. Accessed 3 Oct. 2018. The authors welcome a robust discussion on how these metrics could be improved and have made recommendations for the same in this report.
- 10 Newman, Craig A. "When to Report a Cyberattack? For Companies, That's Still a Dilemma." The New York Times, The New York Times, 5 Mar. 2018, www.nytimes.com/2018/03/05/business/dealbook/sec-cybersecurity-guidance.html. Accessed 19 Oct. 2018.
- 11 "CEA Report: The Cost of Malicious Cyber Activity to the U.S. Economy." The White House, The United States Government, 16 Feb. 2018, www.whitehouse.gov/articles/cea-report-cost-malicious-cyber-activity-u-s-economy/. Accessed 19 Oct. 2018.
- 12 "Clearances." FBI, Federal Bureau of Investigation, 25 Aug. 2017, ucr.fbi.gov/crime-in-the-u.s/2016/crime-in-the-u.s.-2016/topic-pages/clearances. Accessed 19 Oct. 2018.
- 13 Office of Financial Research. "2017 Annual Report to Congress." 29 Sept. 2017, pp. 6. <https://www.financialresearch.gov/annual-reports/files/office-of-financial-research-annual-report-2017.pdf>. Accessed Oct. 3, 2018.
- 14 Cisco. "VNI Complete Forecast Highlights Global Internet Users: % of Population Devices and Connections per Capita Average Speeds Average Traffic per Capita per Month Global -Device Growth Traffic Profiles 2021 Forecast," 2016, pp. 6-7. https://www.cisco.com/c/dam/m/en_us/solutions/service-provider/vni-forecast-highlights/pdf/Global_Device_Growth_Traffic_Profiles.pdf. Accessed 21 Oct. 2018.
- 15 Federal Bureau of Investigation. "2016 Internet Crime Report." 22 June 2017, pp. 14. https://pdf.ic3.gov/2016_IC3Report.pdf. Accessed 3 Oct. 2018.

- 16 This number includes incidents that involve a systemic or targeted breach of a system and does not include privacy crimes, online harassment, or crimes against children. See: Federal Bureau of Investigation. "2016 Internet Crime Report." 22 June 2017, pp. 2. https://pdf.ic3.gov/2016_IC3Report.pdf. Accessed 3 Oct. 2018.
- 17 Federal Bureau of Investigation. "2016 Internet Crime Report." 22 June 2017, pp. 17. https://pdf.ic3.gov/2016_IC3Report.pdf. Accessed 3 Oct. 2018.
- 18 Federal Bureau of Investigation. "2017 Crime in the United States," 2017. <https://ucr.fbi.gov/crime-in-the-u.s/2017/crime-in-the-u.s.-2017/topic-pages/burglary>. Accessed 24 Sept. 2018.
- 19 Federal Bureau of Investigation. "Filing a Complaint with the IC3." <https://www.ic3.gov/about/default.aspx>. Accessed 3 Oct. 2018.
- 20 Federal Bureau of Investigation. "2017 Internet Crime Report." 7 May 2018, pp. 4. https://pdf.ic3.gov/2017_IC3Report.pdf. Accessed 3 Oct. 2018.
- 21 Verizon. "2018 Data Breach Investigations Report (DBIR)." Verizon Bus. J., 10 April 2018, pp. 4. <https://www.verizonenterprise.com/verizon-insights-lab/dbir/>. Accessed 9 Oct. 2018.
- 22 INTERPOL. "Crime Areas | Cybercrime." INTERPOL, 2018. <https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime>. Accessed 9 Oct. 2018.
- 23 United States Department of Justice, Office of Legal Education, "Prosecuting Computer Crimes," 1 Jan. 2015, pp. V. <https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf>. Accessed 3 Oct. 2018.
- 24 Wolff, Josephine. "Why We Need to Be Much More Careful About How We Use the Word Cyberattack." Slate Magazine, Slate Magazine, 30 Mar. 2017, www.slate.com/blogs/future_tense/2017/03/30/we_should_be_careful_when_we_use_the_word_cyberattack.html. Accessed 9 Oct. 2018.
- 25 Federal Bureau of Investigation, "WHAT WE INVESTIGATE; Cyber Crime." <https://www.fbi.gov/investigate/cyber>. Accessed 3 Oct. 2018.
- 26 Wray, Christopher. "Statement Before the Senate Homeland Security and Government Affairs Committee," 27 Sept. 2017. <https://www.fbi.gov/news/testimony/current-threats-to-the-homeland>. Accessed 3 Oct. 2018.
- 27 United States Department of Justice, "Report of the Attorney General's Cyber Digital Task Force." 2 July 2018, pp. 31. <https://www.justice.gov/ag/page/file/1076696/download>. Accessed 3 Oct. 2018.
- 28 Ellis, Emma Grey. "Doxing Is a Perilous Form of Justice-Even When It's Outing Nazis." Wired, Conde Nast, 18 Aug. 2017, www.wired.com/story/doxing-charlottesville/. Accessed 21 Oct. 2018.
- 29 Sanger, David E., and Katie Benner. "U.S. Accuses North Korea of Plot to Hurt Economy as Spy Is Charged in Sony Hack." The New York Times, The New York Times, 6 Sept. 2018, www.nytimes.com/2018/09/06/us/politics/north-korea-sony-hack-wannacry-indictment.html. Accessed 3 Oct. 2018.
- 30 Coats, Daniel R. "WORLDWIDE THREAT ASSESSMENT of the US INTELLIGENCE COMMUNITY." Office of the Director of National Intelligence, Office of the Director of National Intelligence, 13 Feb. 2018, www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf. Accessed 21 Oct. 2018.
- 31 United States Department of Justice. "Report of the Attorney General's Cyber Digital Task Force." July 2, 2018, pp. 32-33. <https://www.justice.gov/ag/page/file/1076696/download>. Accessed 3 Oct. 2018.
- 32 Accenture. "2017 Cost of Cyber Crime Study." 26 Sept. 2017, pp. 23. <https://www.accenture.com/us-en/insight-cost-of-cybercrime-2017>. Accessed 3 Oct. 2018.
- 33 Symantec. "2018 Internet Security Threat Report." 20 March 2018. <https://www.symantec.com/security-center/threat-report>. Accessed 3 Oct. 2018.
- 34 Symantec. "2018 Internet Security Threat Report." 20 March 2018. <https://www.symantec.com/security-center/threat-report>. Accessed 3 Oct. 2018.

- 35 Ponemon Institute LLC. "2017 Cost of Data Breach Study, Global Overview." IBM, June 2017, pp. 1. <https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN>, Accessed 3 Oct. 2018.
- 36 Federal Bureau of Investigation. "2017 Internet Crime Report." 7 May 2018, pp. 17. https://pdf.ic3.gov/2017_IC3Report.pdf, Accessed 3 Oct 2018.
- 37 United States White House, The Council of Economic Advisers. "The Cost of Malicious Cyber Activity to the U.S. Economy." February 2018, pp. 1. <https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf>, Accessed 3 Oct 2018.
- 38 Sterling, Bruce. "Global Cybercrime Costs a Trillion Dollars. Maybe 3." Wired, Conde Nast, 19 July 2017, www.wired.com/beyond-the-beyond/2017/07/global-cybercrime-costs-trillion-dollars-maybe-3/, Accessed 3 Oct. 2018.
- 39 Verizon. "2018 Data Breach Investigations Report (DBIR)." Verizon Bus. J., 10 April 2018, pp. 25. <https://www.verizonenterprise.com/verizon-insights-lab/dbir/>, Accessed 9 Oct. 2018.
- 40 Thielman, Sam, and Chris Johnston. "Major Cyber Attack Disrupts Internet Service across Europe and US." The Guardian, Guardian News and Media, 21 Oct. 2016, www.theguardian.com/technology/2016/oct/21/ddos-attack-dyn-internet-denial-service, Accessed 3 Oct. 2018.
- 41 Wexler, Chuck. "New National Commitment Required: The Changing Nature of Crime and Criminal Investigations." Police Executive Research Forum, January 2018, pp. 4. <https://www.policeforum.org/assets/ChangingNatureofCrime.pdf>, Accessed 3 Oct. 2018.
- 42 Tor is a special kind of web browser commonly used to access the dark web designed for user anonymity. Inc. "Tor." Tor Browser. www.torproject.org/projects/torbrowser.html.en, Accessed 22 Oct. 2018.
- 43 The dark web is content on the Internet that requires special anonymizing software to access. Websites may additionally require specific authorization from administrators and are commonly used by individuals who seek privacy for a variety of reasons. Eddy, Max. "Inside the Dark Web." PCMag, PCMag, 4 Feb. 2015, www.pcmag.com/article2/0,2817,2476003,00.asp, Accessed 22 Oct. 2018.
- 44 Federal Bureau of Investigation. "2017 Internet Crime Report." 7 May 2018, pp. 19. Accessed Oct. 3, 2018. https://pdf.ic3.gov/2017_IC3Report.pdf, Accessed 3 Oct. 2018.
- 45 Federal Bureau of Investigation. "2017 Internet Crime Report." 7 May 2018, pp. 19. Accessed Oct. 3, 2018. https://pdf.ic3.gov/2017_IC3Report.pdf, Accessed 3 Oct. 2018.
- 46 Berr, Jonathan. "'WannaCry' Ransomware Attack Losses Could Reach \$4 Billion." CBS News, CBS Interactive, 16 May 2017, www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/, Accessed 3 Oct. 2018.
- 47 United States Department of Homeland Security. "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors." 15 March 2018. <https://www.us-cert.gov/ncas/alerts/TA18-074A>, Accessed Oct. 3 2018.
- 48 Verizon. "Data breach digest." pp 39. http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest_xg_en.pdf, Accessed 10 Oct. 2018.
- 49 Nakashima, Ellen, and Paul Sonne. "China Hacked a Navy Contractor and Secured a Trove of Highly Sensitive Data on Submarine Warfare." The Washington Post, WP Company, 8 June 2018, www.washingtonpost.com/world/national-security/china-hacked-a-navy-contractor-and-secured-a-trove-of-highly-sensitive-data-on-submarine-warfare/2018/06/08/08/6cc396fa-68e6-11e8-bea7-c8eb28bc52b1_story.html?utm_term=.49fd1da664, Accessed 9 Oct. 2018.
- 50 The Commission on the Theft of American Intellectual Property. "The Report of the Commission on the Theft of American Intellectual Property." The National Bureau of Asian Research, Feb. 2017, pp.1 http://ipcommission.org/report/IP_Commission_Report_Update_2017.pdf, Accessed 10 Oct. 2018.

- 51 Nakashima, Ellen. "Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say." The Washington Post, WP Company, 9 July 2015, www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/. Accessed 22 Oct. 2018.
- 52 Mazzetti, Mark, and Katie Benner. "12 Russian Agents Indicted in Mueller Investigation." The New York Times, The New York Times, 13 July 2018, www.nytimes.com/2018/07/13/us/politics/mueller-indictment-russian-intelligence-hacking.html. Accessed 9 Oct. 2018.
- 53 The enforcement rate was calculated using 2016 IC3 data instead of the most recent for 2017 due to the fact that is the most recent year of reported UCR statistics. Federal Bureau of Investigation. "2016 Internet Crime Report." 22 June 2017. https://pdf.ic3.gov/2016_IC3Report.pdf. Accessed 3 Oct. 2018.
- 54 Federal Bureau of Investigation. "2015 Crime in the United States: federal Crime Data." 26 Sept. 2016. https://ucr.fbi.gov/crime-in-the-u.s/2015/crime-in-the-u.s.-2015/additional-reports/federal-crime-data/federal_crime_data_-_2015. Accessed 3 Oct. 2018; Federal Bureau of Investigation. "2014 Crime in the United States: Federal Crime Data, 2014." 28 Sept. 2015. <https://ucr.fbi.gov/about-us/cjis/ucr/crime-in-the-u.s/2014/crime-in-the-u.s.-2014/additional-reports/federal-crime-data/federal-crime-data.pdf>. Accessed 3 Oct. 2018.
- 55 "2016 NIBRS Crime data Released." Federal Bureau of Investigation, 11 Dec. 2017. <https://www.fbi.gov/news/stories/2016-nibrs-data-released>. Accessed 3 Oct. 2018.
- 56 United States Secret Service. "Presidential Campaign 2016 Annual Report." pp. 14. https://www.secretsservice.gov/data/press/reports/USSS_FY2016AR.pdf. Accessed 10 Oct. 2018.
- 57 Federal Bureau of Investigation. "2016 Internet Crime Report." 22 June 2017, pp. 2. https://pdf.ic3.gov/2016_IC3Report.pdf. Accessed Oct. 3, 2018.
- 58 Baker, Al. "An 'Iceberg' of Unseen Crimes: Many Cyber Offenses Go Unreported." The New York Times, The New York Times, 5 Feb. 2018, www.nytimes.com/2018/02/05/nyregion/cyber-crimes-unreported.html. Accessed 10 Oct. 2018; Wexler, Chuck. "New National Commitment Required: The Changing Nature of Crime and Criminal Investigations." Police Executive Research Forum, Jan. 2018. <https://www.policeforum.org/assets/ChangingNatureofCrime.pdf>. Accessed Oct. 3, 2018.
- 59 Federal Bureau of Investigation. "FY 2018 Authorization and Budget Request to Congress." May 2017, pp 4-31. <https://www.justice.gov/file/968931/download>. Accessed 5 Oct. 2018.
- 60 Federal Bureau of Investigation. "FY 2018 Authorization and Budget Request to Congress." May 2017, pp 4-31. <https://www.justice.gov/file/968931/download>. Accessed 5 Oct. 2018.
- 61 Sulemeyer, Michael. "Why the U.S. Should switch from Cyber-Deterrence to Playing Cyber-Offense." Foreign Affairs, 22 March 2018. <https://www.foreignaffairs.com/articles/world/2018-03-22/how-us-can-play-cyber-offense>. Accessed 5 Oct. 2018.
- 62 Baker, Stewart, and Victoria Muth. "Should Companies Risk Going on the Cyber Offensive?" Brink – The Edge of Risk, Marsh & McLennan Companies' Global Risk Center, 22 July 2016, www.brinknews.com/should-companies-risk-going-on-the-cyber-offensive/. Accessed 5 Oct. 2018.
- 63 National Academies of Sciences. "Modernizing Crime Statistics: Report 1: Defining and Classifying Crime." The National Academies Press, 16 May 2016. doi.org/10.17226/23492. Accessed 22 Oct. 2018.
- 64 Mazzetti, Mark, and Katie Benner. "12 Russian Agents Indicted in Mueller Investigation." The New York Times, The New York Times, 13 July 2018, www.nytimes.com/2018/07/13/us/politics/mueller-indictment-russian-intelligence-hacking.html. Accessed 5 Oct. 2018; Starks, Tim. "U.S. Indicts North Korean National for Sony Hack, Massive Cyberattacks." POLITICO, POLITICO Magazine, 6 Sept. 2018, www.politico.com/story/2018/09/06/justice-department-north-korea-sony-hack-771212. Accessed 5 Oct. 2018.
- 65 Healey, Jason. "Beyond Attribution: Seeking National Responsibility for Cyber Attacks." The Atlantic Council, pp. 2-4. January 2012. https://www.bjic.gov/public/2012/mar/National_Responsibility_for_CyberAttacks_2012.pdf. Accessed 10 Oct. 2018.

- 66 Mathews, Lee. "Equifax Data Breach Impacts 143 Million Americans," *Forbes Magazine*, 7 Sept. 2017. <https://www.forbes.com/sites/leemathews/2017/09/07/equifax-data-breach-impacts-143-million-americans/#6f153672356f>. Accessed 9 Oct. 2018.
- 67 Nakashima, Ellen. "White House Declassifies Outline of Cybersecurity Program." *The Washington Post*, WP Company, 3 Mar. 2010. www.washingtonpost.com/wpdyn/content/article/2010/03/02/AR2010030202113.html. Accessed 5 Oct. 2018.
- 68 United States White House. "The Comprehensive National Cybersecurity Initiative." 15 July 2015. <https://web.archive.org/web/2010071523803/www.whitehouse.gov/sites/default/files/Cybersecurity.pdf>. Accessed 5 Oct. 2018.
- 69 United States White House. "The Comprehensive National Cybersecurity Initiative." 15 July 2015. <https://web.archive.org/web/2010071523803/www.whitehouse.gov/sites/default/files/Cybersecurity.pdf>. Accessed 5 Oct. 2018.
- 70 United States White House, National Security Council. "President Trump Unveils America's First Cybersecurity Strategy in 15 Years." 20 Sept. 2018. <https://www.whitehouse.gov/articles/president-trump-unveils-americas-first-cybersecurity-strategy-15-years/>. Accessed Oct. 9, 2018.
- 71 MacLellan, Stephanie, and Naomi O'Leary. "Doing Battle in Cyberspace: How an Attack on Estonia Changed the Rules of the Game." *Centre for International Governance Innovation*, Centre for International Governance Innovation, 26 Oct. 2017. www.cigionline.org/articles/doing-battle-cyberspace-how-attack-estonia-changed-rules-game. Accessed 27 Oct. 2018; United States, Congress, House, Armed Services Committee. "Cyber Warfare in the 21st Century: Threats, Challenges, and Opportunities." Government Printing Office, 1 March 2017. 115th Congress, 1st session, House Report [115-8]. <https://www.gpo.gov/fdsys/pkg/CHRG-115hhrg24680/pdf/CHRG-115hhrg24680.pdf>. Accessed 9 Oct. 2018.
- 72 NATO Cooperation Cyber Defence Center of Excellence. "Tallinn Manual Process." <https://ccdcoe.org/tallinn-manual.html>. Accessed 10 Oct. 2018.
- 73 Smith, Brad. "The need for a Digital Geneva Convention," RSA Conference, San Francisco, CA, 14 Feb. 2017. <https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/>. Accessed 10 Oct. 2018.
- 74 United States White House. "Statement by President Donald J. Trump on the Elevation of Cyber Command." 18 Aug. 2017. <https://www.whitehouse.gov/briefings-statements/statement-president-donald-j-trump-elevation-cyber-command/>. Accessed Oct. 9, 2018.
- 75 Pomerleau, Mark. "CYBERCOM elevation at heart of budget increase." *Defense News*, 24 May 2017. <https://www.defensenews.com/2017/05/24/cybercom-elevation-at-heart-of-budget-increase/>. Accessed 9 Oct. 2018.
- 76 Volz, Dustin. "Trump, Seeking to Relax Rules on U.S. cyberattacks, Reverses Obama Directive." *The Wall Street Journal*, 15 Aug. 2018. <https://www.wsj.com/articles/trump-seeking-to-relax-rules-on-u-s-cyberattacks-reverses-obama-directive-1534378721>. Accessed 9 Oct. 2018.
- 77 Nakashima, Ellen, and Adam Goldman. "In a First, Chinese Hackers Are Arrested at the Behest of the U.S. Government." *The Washington Post*, WP Company, 9 Oct. 2015. www.washingtonpost.com/world/national-security/in-a-first-chinese-hackers-are-arrested-at-the-behest-of-the-us-government/2015/10/09/0a7b0e46-6778-11e5-8325-a42b5a459b1e_story.html?postshare=9811444395972124&utm_term=.dfca74bada27. Accessed 9 Oct. 2018.
- 78 Leyden, John. "China Cuffs Hackers at US Request to Stave off Sanctions." *The Register*® - Biting the Hand That Feeds IT, *The Register*, 9 Oct. 2015. www.theregister.co.uk/2015/10/09/china_cuffs_hackers_at_us_request/. Accessed 9 Oct. 2018.
- 79 United States District Court for the District of Columbia. "United States of America v. Viktor Borisovich Netyksho Et Al." *New York Times*, 13 July 2018. int.nyt.com/data/documenthelper/80-netyksho-et-al-indictment/ba0521c1eef869deecbe/optimized/full.pdf?action=click&module=Intentional&pgtype=Article. Accessed 22 Oct. 2018.

- 80 Deputy Attorney General Rod J. Rosenstein. "Remarks at the Aspen Security Forum," Aspect Security Forum. "19 July 2018. <https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-aspen-security-forum>. Accessed 9 Oct. 2018.
- 81 "Federal Budget Cyber Security Spending." White House, 2016. https://www.whitehouse.gov/wp-content/uploads/2018/02/ap_21_cyber_security-fy2019.pdf. Accessed 9 Oct. 2018.
- 82 Carter, William A. and Jennifer C. Daskal. "Low-Hanging Fruit: Evidence Based Solutions to the Digital Evidence Challenge." Center for Strategic & International Studies, July 2018. <https://www.csis.org/analysis/low-hanging-fruit-evidence-based-solutions-digital-evidence-challenge>. Accessed Oct. 9, 2018.
- 83 Carter, William A. and Jennifer C. Daskal. "Low-Hanging Fruit: Evidence Based Solutions to the Digital Evidence Challenge." Center for Strategic & International Studies, July 2018, pp. 5. <https://www.csis.org/analysis/low-hanging-fruit-evidence-based-solutions-digital-evidence-challenge>. Accessed Oct. 9, 2018; United States Secret Service. "2017 Annual Report." 2017, pp. 21. https://www.secretservice.gov/data/press/reports/CMR-2017_Annual_Report_online.pdf. Accessed 9 Oct. 2018.
- 84 Carter, William A. and Jennifer C. Daskal. "Low-Hanging Fruit: Evidence Based Solutions to the Digital Evidence Challenge." Center for Strategic & International Studies, July 2018, pp. 5. <https://www.csis.org/analysis/low-hanging-fruit-evidence-based-solutions-digital-evidence-challenge>. Accessed Oct. 9, 2018.
- 85 Carter, William A. and Jennifer C. Daskal. "Low-Hanging Fruit: Evidence Based Solutions to the Digital Evidence Challenge." Center for Strategic & International Studies, July 2018, pp. 14. <https://www.csis.org/analysis/low-hanging-fruit-evidence-based-solutions-digital-evidence-challenge>. Accessed Oct. 9, 2018.
- 86 Carter, William A. and Jennifer C. Daskal. "Low-Hanging Fruit: Evidence Based Solutions to the Digital Evidence Challenge." Center for Strategic & International Studies, July 2018, pp. 9. <https://www.csis.org/analysis/low-hanging-fruit-evidence-based-solutions-digital-evidence-challenge>. Accessed Oct. 9, 2018.
- 87 Taylor, Michelle. "New York City Opens its \$10 Million Cybercrime Lab." Forensic Magazine, 17 Nov. 2016. <https://www.forensicmag.com/news/2016/11/new-york-city-opens-its-10-million-cybercrime-lab>. Accessed 10 Oct. 2018.
- 88 Carter, William A. and Jennifer C. Daskal. "Low-Hanging Fruit: Evidence Based Solutions to the Digital Evidence Challenge." Center for Strategic & International Studies, July 2018, pp. 12. <https://www.csis.org/analysis/low-hanging-fruit-evidence-based-solutions-digital-evidence-challenge>. Accessed 9 Oct. 2018.
- 89 Digital evidence is "information stored or transmitted in binary form that may be relied on in court." It can be found on such things as a computer hard drive or a mobile phone and is used to prosecute a wide spectrum of crimes. United States Department of Justice, Office of Justice Programs. "Digital Evidence and Forensic." National Institute of Justice, 14 April 2016. <https://www.nij.gov/topics/forensics/evidence/digital/Pages/welcome.aspx>. Accessed 9 Oct. 2018.
- 90 Secretary of Commerce Wilbur Ross and Acting Secretary of Homeland Security Elaine Duke. "A Report to the President on Supporting the Growth and Sustainment of the nation's Cybersecurity Workforce: Building the foundation for a More Secure American Future." 30 May 2018, pp. 1. https://www.dhs.gov/sites/default/files/publications/eo_wf_report_to_potus.pdf. Accessed 9 Oct. 2018.
- 91 Hurley, Deborah. "Improving Cybersecurity: The Diversity Imperative." Forbes. Forbes Magazine, 7 May 2017. <https://www.forbes.com/sites/ciocentral/2017/05/07/improving-cybersecurity-the-diversity-imperative/#1fb6a901e30>. Accessed 19 Oct. 2018.
- 92 United States Department of Justice, Office of the Inspector General. "Audit of the Federal Bureau of Investigation's Implementation of Its Next Generation Cyber Initiative." July 2015, pp. ii. <https://oig.justice.gov/reports/2015/a1529.pdf>. Accessed 9 Oct. 2018.

- 93 United States Department of Justice, Office of the Inspector General. "Audit of the Federal Bureau of Investigation's Implementation of Its Next Generation Cyber Initiative." July 2015, pp. 8. <https://oig.justice.gov/reports/2015/a1529.pdf>. Accessed 9 Oct. 2018.
- 94 Geller, Eric. "FBI Struggles to Retain Top Cyber Talent." POLITICO, POLITICO Magazine, 3 Aug. 2018, www.politico.com/story/2018/08/03/fbi-cyber-security-talent-drain-hacking-threat-russia-elections-760740. Accessed 10 Oct. 2018.
- 95 Wexler, Chuck. "New National Commitment Required: The Changing Nature of Crime And Criminal Investigations." Police Executive Research Forum, January 2018, pp. 59. <https://www.policeforum.org/assets/ChangingNatureofCrime.pdf>. Accessed 9 Oct. 2018.
- 96 Carter, William A. and Jennifer C. Daskal. "Low-Hanging Fruit: Evidence Based Solutions to the Digital Evidence Challenge." Center for Strategic & International Studies, July 2018, pp.4. <https://www.csis.org/analysis/low-hanging-fruit-evidence-based-solutions-digital-evidence-challenge>. Accessed 9 Oct. 2018.
- 97 Berghel, Hal. "On the Problem of (Cyber) Attribution." Computer, vol. 62, no. 47, 2017, pp. 84–89. <https://ieeexplore.ieee.org/document/7888425>. Accessed 22 Oct. 2018.
- 98 "Machine Learning: Practical Applications for Cybersecurity." Recorded Future, 14 Mar. 2018, www.recordedfuture.com/machine-learning-cybersecurity-applications/. Accessed 22 Oct. 2018.
- 99 Zetter, Kim. "Apple's FBI Battle Is Complicated. Here's What's Really Going On." Wired, Conde Nast, 3 June 2017, www.wired.com/2016/02/apples-fbi-battle-is-complicated-heres-whats-really-going-on/. Accessed 19 Oct. 2018.
- 100 Newman, Lily Hay. "Why Is It So Hard to Prove Russia Hacked the DNC?" Wired, Conde Nast, 3 June 2017, www.wired.com/2016/12/hacker-lexicon-attribution-problem/. Accessed 19 Oct. 2018.
- 101 Wheeler, David A., and Gregory N. Larsen. "Techniques for Cyber Attack Attribution." Institute for Defense Analysis, Jan. 2003, pp 2, doi.org/10.21236/ada468859. Accessed 19 Oct. 2018.
- 102 Tran, Delbert. "The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack." Yale Journal of Law & Technology, vol. 20, no. 376, May 10 2017, pp. 3–4., www.yjolt.org/sites/default/files/2017/05/yale_j_l_tech_376.pdf. Accessed 19 Oct. 2018.
- 103 "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage." The United States Department of Justice, 22 July 2015, www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor. Accessed 19 Oct. 2018; "U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations." The United States Department of Justice, 4 Oct. 2018, www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and. Accessed 19 Oct. 2018.
- 104 Collier, Kevin. "The Indictment Of North Korea For The Sony Hack Shows How Cybersecurity Has Evolved." BuzzFeed News, BuzzFeed, 10 Sept. 2018, www.buzzfeednews.com/amphtml/kevincollier/the-indictment-of-north-korea-for-the-sony-hack-shows-how. Accessed 19 Oct. 2018.
- 105 Biddle, Sam. "Here's the Public Evidence Russia Hacked the DNC - It's Not Enough." The Intercept, 14 Dec. 2016, www.theintercept.com/2016/12/14/heres-the-public-evidence-russia-hacked-the-dnc-its-not-enough/. Accessed 19 Oct. 2018.
- 106 Apuzzo, Matt, and Sharon Lafraniere. "13 Russians Indicted as Mueller Reveals Effort to Aid Trump Campaign." The New York Times, The New York Times, 16 Feb. 2018, www.nytimes.com/2018/02/16/us/politics/russians-indicted-mueller-election-interference.html. Accessed 19 Oct. 2018.
- 107 Lynch, Justin. "America Could Protect Cyberspace like WMDs." Fifth Domain, Fifth Domain, 1 Aug. 2018, www.fifthdomain.com/civilian/2018/08/01/america-could-protect-cyberspace-like-wmds/. Accessed 19 Oct. 2018.
- 108 Crerar, Pippa, et al. "Russia Accused of Cyber-Attack on Chemical Weapons Watchdog." The Guardian, Guardian News and Media, 4 Oct. 2018, www.theguardian.com/world/2018/oct/04/netherlands-halted-russian-cyber-attack-on-chemical-weapons-body. Accessed 19 Oct. 2018.

- 109 The Office of the President of the United States. National Cyber Strategy of the United States of America. The White House, September, 2018. Available at: <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>. Accessed 19 Oct. 2018.
- 110 "Most Wanted." FBI, Federal Bureau of Investigation, 3 May 2016, www.fbi.gov/investigate/cyber/most-wanted. Accessed 19 Oct. 2018.
- 111 "Ten Most Wanted Fugitives FAQ." FBI, Federal Bureau of Investigation, 17 Sept. 2010, www.fbi.gov/wanted/top10/ten-most-wanted-fugitives-faq. Accessed 19 Oct. 2018.
- 112 "Ten Most Wanted Fugitives FAQ." FBI, Federal Bureau of Investigation, 17 Sept. 2010, www.fbi.gov/wanted/top10/ten-most-wanted-fugitives-faq. Accessed 19 Oct. 2018.
- 113 "Ten Most Wanted Fugitives FAQ." FBI, Federal Bureau of Investigation, 17 Sept. 2010, www.fbi.gov/wanted/top10/ten-most-wanted-fugitives-faq. Accessed 19 Oct. 2018.
- 114 "New Top Ten Fugitive." FBI, Federal Bureau of Investigation, 27 Sept. 2018, www.fbi.gov/news/stories/new-top-ten-fugitive-greg-alyn-carlson-092718. Accessed 19 Oct. 2018.
- 115 "Sanctions Related to Significant Malicious Cyber-Enabled Activities." U.S. Department of the Treasury, www.treasury.gov/resource-center/sanctions/Programs/Pages/cyber.aspx. Accessed 19 Oct. 2018.
- 116 OFAC administers and enforces an extensive range of US trade and economic sanctions that target individuals, entities, and entire governments. Office of Foreign Assets Control. "Cyber-Related Sanctions Program," U.S. Department of the Treasury, 3 July 2017, pp 6. <https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber.pdf>. Accessed 19 Oct. 2018.
- 117 Executive Order. No. 13757, 2016, p. 1. https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber2_eo.pdf. Accessed 19 Oct. 2018.
- 118 "Sanctions Programs and Country Information." U.S. Department of the Treasury, www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx. Accessed 19 Oct. 2018.
- 119 United States Congress, House, "Countering America's Adversaries Through Sanctions Act." Congress.gov, <https://www.congress.gov/bills/115/congress/house-bill/3364>. 115th Congress, 1st session, House Resolution 3364, passed Aug. 02, 2017.
- 120 Masters, Jonathan. "What Are Economic Sanctions?" Council on Foreign Relations, Council on Foreign Relations, 7 Aug. 2017, www.cfr.org/backgrounder/what-are-economic-sanctions. Accessed Oct. 9, 2018.
- 121 See generally, Stoll, Cliff. Cuckoos Egg. Doubleday, 1989.
- 122 Carter, William A. and Jennifer C. Daskal. "Low-Hanging Fruit: Evidence Based Solutions to the Digital Evidence Challenge." Center for Strategic & International Studies, July 2018, pp. 5. <https://www.csis.org/analysis/low-hanging-fruit-evidence-based-solutions-digital-evidence-challenge>. Accessed Oct. 9, 2018.
- 123 Chalfant, Morgan. "State Dept. to Eliminate Cyber Office: Report." TheHill, 19 July 2017, thehill.com/policy/cybersecurity/342698-state-dept-to-eliminate-cyber-office-report. Accessed 19 Oct. 2018.
- 124 Johnson, Derek B. "Senate Panel Votes to Revive State Cyber Office." FCW, fcw.com/articles/2018/06/26/cyber-state-senate-office.aspx. Accessed 19 Oct. 2018.
- 125 Cohen, Zachary, et al. "Trump's Attacks Leave NATO Allies in Disbelief." CNN, Cable News Network, 12 July 2018, www.cnn.com/2018/07/11/politics/trump-nato-diplomats-reaction/index.html. Accessed 19 Oct. 2018.
- 126 The full list of countries that the United States has signed MLATs and agreed upon MLAs with can be found here: "Treaties and Agreements." U.S. Department of State, U.S. Department of State, 7 Mar. 2012, www.state.gov/j/inl/rls/nrcrpt/2012/vol2/184110.htm. Accessed 19 Oct. 2018.
- 127 Mulligan Stephen, "Cross-Border Data Sharing Under the CLOUD Act," Congressional Research Service, 23 Apr., 2018, pp 15-23. <https://fas.org/srg/crs/misc/R45173.pdf>. Accessed 19 Oct. 2018.
- 128 Mulligan Stephen, "Cross-Border Data Sharing Under the CLOUD Act," Congressional Research Service, 23 Apr., 2018, pp 15-23. <https://fas.org/srg/crs/misc/R45173.pdf>. Accessed 19 Oct. 2018.

- 129 United States Congress, House, "CLOUD Act." Congress.gov,<https://www.congress.gov/bill/115th-congress/house-bill/4943> 115th Congress, 2nd session, House Resolution 4934, introduced Feb. 6, 2018, as included in United States Congress, House, "Consolidated Appropriations Act, 2018," Congress.gov, <https://www.congress.gov/bill/115th-congress/house-bill/1625>, 115th Congress, 2nd session, House Resolution 1625, passed March 3, 23, 2018.
- 130 United States Department of Justice, "Interpol Red Notices," Sept. 19, 2018. Accessed Oct. 10, 2018. Available at: <https://www.justice.gov/im/criminal-resource-manual-611-interpol-red-notices>; "Red Notices." Red Notices / Notices / INTERPOL Expertise / Internet / Home – INTERPOL, www.interpol.int/INTERPOL-expertise/Notices/Red-Notices.
- 131 "Interpol Red Notices." Criminal Resource Manual, The United States Department of Justice, 19 Sept. 2018, www.justice.gov/im/criminal-resource-manual-611-interpol-red-notices. Accessed 19 Oct. 2018.
- 132 Doyle, Charles. "An Abridged Sketch of Extradition To and From the United States.", Congressional Research Service, 4 Oct. 2016. RS22702, fas.org/sgp/crs/misc/RS22702.pdf. Accessed 19 Oct. 2018.
- 133 "Convention on Cybercrime." Treaty Office, Council of Europe, www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185. Accessed 19 Oct. 2018.
- 134 The Office of the President of the United States. National Cyber Strategy of the United States of America. The White House, September, 2018, pp 26. Available at: <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>. Accessed 19 Oct. 2018.
- 135 Office of the Coordinator For Cyber Issues. "Cybercrime Factsheet." United States Department of State, A/GIS/GPS, Aug. 2015, 2009-2017, state.gov/documents/organization/255007.pdf. Accessed 19 Oct. 2018.
- 136 For example, the International Criminal Investigative Training Assistance Program (ICITAP) at the US Department of Justice provides technical assistance and training to foreign governments to fight transnational cybercrime. "Terrorism and Transnational Crime." The United States Department of Justice, 10 Feb. 2016, www.justice.gov/criminal-icitap/subject-matter-expertise/terrorism-transnational-crime. Accessed 19 Oct. 2018.
- 137 Norris, John. "A Bad Budget for America's Place in the World." Center for American Progress, 13 Feb. 2018, www.americanprogress.org/issues/security/news/2018/02/13/446557/bad-budget-americas-place-world/. Accessed 19 Oct. 2018.
- 138 Corrigan, Jack, and Government Executive. "The Hollowing Out of the State Department Continues." The Atlantic, Atlantic Media Company, 11 Feb. 2018, www.theatlantic.com/international/archive/2018/02/tillerson-trump-state-foreign-service/553034/. Accessed 19 Oct. 2018.
- 139 The Office of the President of the United States. National Cyber Strategy of the United States of America. The White House, September, 2018. Available at: <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>. Accessed 19 Oct. 2018.
- 140 See for example, Data Protection and Cybercrime Division, Council of Europe. "Capacity Building on Cybercrime." Council of Europe, 2013, [doi:10.1017/CBO9781107415324.004](https://doi.org/10.1017/CBO9781107415324.004). Accessed 19 Oct. 2018.
- 141 "Activities." Capacity Building / Activities / Cybercrime / Crime Areas / Internet / Home – INTERPOL, www.interpol.int/Crime-areas/Cybercrime/Activities/Capacity-building. Accessed 19 Oct. 2018.
- 142 "Capacity Building for Criminal Justice Practitioners Combating Cybercrime and Cyber-Enabled Crime in South-Eastern Europe." OSCE POLIS, Organization for Security and Co-Operation, polis.osce.org/node/9381. Accessed 19 Oct. 2018.
- 143 See for example "Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy." Freedom House, 31 Aug. 2018, www.freedomhouse.org/report/freedom-net/freedom-net-2017; Waterman, Shaun. "Freedom House: Governments Are Turning Cyberweapons on Their Own People." Cyberscoop, 14 Nov. 2017, www.cyberscoop.com/freedom-house-repression-fotn-cyberweapons-ddos-dissidents/. Accessed 19 Oct. 2018

- 144 For example, Egypt recently passed a new cybercrime law that human rights groups argue allows broad scope for the Egyptian government to prosecute journalists, activists, and government critics for any criticism of the government: "Egypt Internet: Sisi Ratifies Law Tightening Control over Websites." BBC News, BBC, 18 Aug. 2018, www.bbc.com/news/world-middle-east-45237171. Accessed 19 Oct. 2018
- 145 Finklea, Kristin, "Justice Department's Role In Cyber Incident Response," Congressional Research Service, August 23, 2017, pp 8-9. <https://fas.org/sgp/crs/misc/R44926.pdf>. Accessed 19 Oct. 2018
- 146 Baker, Al. "An 'Iceberg' of Unseen Crimes: Many Cyber Offenses Go Unreported." The New York Times, 5 Feb. 2018. <https://www.nytimes.com/2018/02/05/nyregion/cyber-crimes-unreported.html>. Accessed 19 Oct. 2018.
- 147 Baker, Al. "An 'Iceberg' of Unseen Crimes: Many Cyber Offenses Go Unreported." The New York Times, 5 Feb. 2018. <https://www.nytimes.com/2018/02/05/nyregion/cyber-crimes-unreported.html>. Accessed 19 Oct. 2018.
- 148 Lauristen, Janet and Cork, Daniel. "Expanding Our Understanding of Crime: The National Academies Report on the Future of Crime Statistics and Measurement." *Criminology and Public Policy*, vol. 16, no. 4, 2017, pp. 1075-98, doi:10.1111/1745-9133.12332.
- 149 Lauristen, Janet and Cork, Daniel. "Expanding Our Understanding of Crime: The National Academies Report on the Future of Crime Statistics and Measurement." *Criminology and Public Policy*, vol. 16, no. 4, 2017, pp. 1075-98, doi:10.1111/1745-9133.12332.
- 150 Federal Bureau of Investigation. FY 2018 Authorization and Budget Request to Congress. Department of Justice. May 2017, pp 4-31. <https://www.justice.gov/file/968931/download>. Accessed 19 Oct. 2018.
- 151 Federal Bureau of Investigation. FY 2018 Authorization and Budget Request to Congress. Department of Justice. May 2017, pp 4-31. <https://www.justice.gov/file/968931/download>. Accessed 19 Oct. 2018.
- 152 United States Secret Service. US Secret Service Budget Overview FY 2019 Congressional Justification. Department of Homeland Security, May 2017, pp 4. <https://www.dhs.gov/sites/default/files/publications/U.S.%20Secret%20Service.pdf>. Accessed 19 Oct. 2018.
- 153 Federal Bureau of Investigation. FY 2018 Authorization and Budget Request to Congress. Department of Justice. May 2017, pp 4-31. <https://www.justice.gov/file/968931/download>. Accessed 19 Oct. 2018.
- 154 United States, Congress, Cong. House, Committee on Oversight and Government Reform. "United States Secret Service: an Agency in Crisis", 9 Dec. 2015. 114th Congress, 1st session, report, [oversight.house.gov/wp-content/uploads/2015/12/Oversight-USSS-Report.pdf](https://www.oversight.house.gov/wp-content/uploads/2015/12/Oversight-USSS-Report.pdf). Accessed 19 Oct. 2018.
- 155 "National Cyber Investigative Joint Task Force." FBI, Federal Bureau of Investigation, 13 June 2016, www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force. Accessed 19 Oct. 2018.
- 156 "Cyber Task Forces: Building Alliances to Improve the Nation's Cybersecurity." FBI, Federal Bureau of Investigation, 31 May 2016, www.fbi.gov/file-repository/cyber-task-forces-fact-sheet.pdf/view. Accessed 19 Oct. 2018.
- 157 "The Investigative Mission." United States Secret Service, www.secretservice.gov/investigation/#field. Accessed 19 Oct. 2018.
- 158 United States Congress, House, "Consolidated Appropriations Act, 2018," Congress.gov, Page 201, <https://www.congress.gov/115/bills/hr/1625/BILLS-115hr1625enr.pdf>. 115th Congress, 2nd session, House Resolution 1625, passed March 23, 2018.
- 159 Dorado, Gene L. "Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation." 2018, pp. 14-18. <https://www.gao.gov/assets/700/693/693405.pdf>. Accessed 19 Oct. 2018.
- 160 The Office of the President of the United States. National Cyber Strategy of the United States of America. The White House, September, 2018. Available at: <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>. Accessed 19 Oct. 2018.

- 161 National Commission on Terrorist Attacks upon the United States. The 9/11 Commission Report. 22 July 2004. www.9-11commission.gov/report/. Accessed 19 Oct. 2018.
- 162 National Commission on Terrorist Attacks upon the United States. The 9/11 Commission Report. 22 July 2004, pp 365. www.9-11commission.gov/report/. Accessed 19 Oct. 2018.
- 163 "Office of National Drug Control Policy." Office of National Drug Control Policy, The White House, www.whitehouse.gov/ondcp/. Accessed 19 Oct. 2018.
- 164 Eilperin, Juliet. "Obama May Appoint an Ebola Czar, He Says." The Washington Post, 16 Oct. 2014, <https://www.washingtonpost.com/news/post-politics/wp/2014/10/16/obama-may-appoint-an-ebola-czar-he-says/>. Accessed 19 Oct. 2018.
- 165 Perloth, Nicole, and David Sanger. "White House Eliminates Cybersecurity Coordinator Role." The New York Times, 15 May 2018, <https://www.nytimes.com/2018/05/15/technology/white-house-cybersecurity.html>. Accessed 19 Oct. 2018.
- 166 Perloth, Nicole, and David Sanger. "White House Eliminates Cybersecurity Coordinator Role." The New York Times, 15 May 2018, <https://www.nytimes.com/2018/05/15/technology/white-house-cybersecurity.html>. Accessed 19 Oct. 2018.
- 167 United States Congress, House, "Consolidated Appropriations Act, 2018," Congress.gov, Page 201, <https://www.congress.gov/115/bills/hr/1625/BILLS-115hr1625enr.pdf>. 115th Congress, 2nd session, House Resolution 1625, passed March 23, 2018.
- 168 Lisa N. Sacco and Kristin Finklea, "The Role of the Office of National Drug Control Policy (ONDCP)," CRS Insight, Congressional Research Service, June 1, 2018, pp 1. <https://fas.org/sgp/crs/misc/INi0912.pdf>. Accessed 19 Oct. 2018.
- 169 "Law Enforcement Cyber Incident Reporting." Department of Justice, www.justice.gov/usao-ct/page/file/906222/download. Accessed 19 Oct. 2018.
- 170 United States, Congress, Cong. House, Committee on Oversight and Government Reform. "United States Secret Service: an Agency in Crisis", 9 Dec. 2015. 114th Congress, 1st session, report, [oversight.house.gov/wp-content/uploads/2015/12/Oversight-USSS-Report.pdf](https://www.oversight.house.gov/wp-content/uploads/2015/12/Oversight-USSS-Report.pdf). Accessed 19 Oct. 2018.
- 171 "Law Enforcement Cyber Incident Reporting." Department of Justice, www.justice.gov/usao-ct/page/file/906222/download. Accessed 19 Oct. 2018.
- 172 "Law Enforcement Cyber Incident Reporting." Department of Justice, www.justice.gov/usao-ct/page/file/906222/download. Accessed 19 Oct. 2018.
- 173 "Law Enforcement Cyber Incident Reporting." Department of Justice, www.justice.gov/usao-ct/page/file/906222/download. Accessed 19 Oct. 2018.
- 174 National Commission on Terrorist Attacks upon the United States. The 9/11 Commission Report. 22 July 2004. www.9-11commission.gov/report/. Accessed 19 Oct. 2018.
- 175 National Commission on Terrorist Attacks upon the United States. The 9/11 Commission Report. 22 July 2004, pp 74. www.9-11commission.gov/report/. Accessed 19 Oct. 2018.
- 176 National Commission on Terrorist Attacks upon the United States. The 9/11 Commission Report. 22 July 2004, pp 76. www.9-11commission.gov/report/. Accessed 19 Oct. 2018.
- 177 National Commission on Terrorist Attacks upon the United States. The 9/11 Commission Report: Executive Summary. 22 July 2004, pp 15-16. www.9-11commission.gov/report/. Accessed October 19, 2018.
- 178 National Commission on Terrorist Attacks upon the United States. The 9/11 Commission Report. 22 July 2004, pp 93-94. www.9-11commission.gov/report/. Accessed 19 Oct. 2018.
- 179 National Commission on Terrorist Attacks upon the United States. The 9/11 Commission Report. 22 July 2004, pp 15-16. www.9-11commission.gov/report/. Accessed 19 Oct. 2018.



About Third Way

Third Way is a nonprofit organization headquartered in Washington, DC. The think tank champions modern center-left ideas and its work is grounded in the mainstream American values of opportunity, freedom, and security.

Third Way's agenda is ambitious, aspirational, and actionable. It is built on the bedrock belief that for political movements to succeed in the US political system, they must relentlessly re-imagine their policies, strategies, and coalitions.

Third Way's advantage lies in its high-impact advocacy campaigns that combine rigorous policy research with a unique and incisive understanding of the vast American middle—the people who ultimately decide majorities and provide mandates for change. The work is designed to persuade elected officials, intellectuals, advocates, the media, and others with political influence.

The Third Way National Security Program is focused on protecting Americans from 21st century global threats by moving forward bold and pragmatic new ideas. The National Security Program works hand in hand with diverse coalitions of civil society groups, academics, and others on all sides of the political spectrum to develop and promote smart and tough policy ideas and educate policymakers to make America strong and safe, while preserving American values. The Program's Cyber Enforcement Initiative is non-partisan and is not associated with any specific US political party.

Letter of Support
Consumer Federation of America
(CFA)
Nov. 13, 2019



Consumer Federation of America

November 13, 2019

The Honorable Maxine Waters
Chairwoman
Financial Services Committee
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Patrick McHenry
Ranking Member
Financial Services Committee
U.S. House of Representatives
Washington, D.C. 20515

Re: The Empowering States to Protect Seniors from Bad Actors Act (Discussion Draft)

Dear Chairwoman Waters, Ranking Member McHenry and Members of the Committee:

We are writing to express our support for the draft legislation entitled “The Empowering States to Protect Seniors from Bad Actors Act,”¹ which would enhance states’ ability to protect seniors from financial exploitation. It would achieve this by clarifying that the senior investor protection grant program authorized by Congress in Section 989(A) of the Dodd-Frank Act to be administered by the Consumer Financial Protection Bureau (CFPB) may be funded in the same manner as all other activities of the CFPB.

Senior financial exploitation is an urgent nationwide concern. It is estimated that roughly one in five citizens over the age of 65, or 7 million seniors, have been victims of financial exploitation. Abuses include inappropriate investment recommendations, unreasonably high fees, and outright fraud,² costing these older Americans an estimated \$2.9 billion.³ Older Americans are particularly hard hit by such practices, since they are often past the point in their earning years where they can recover those losses. And the problem is only expected to intensify with the aging of the “baby boom” generation and with increases to average life expectancies.

State regulators, who form the front line on investor protection for Main Street investors, are an important part of the effort to combat this problem. In recognition of that fact, Section 989(A) of the Dodd-Frank Act established a grant program within the CFPB designed to help state securities and insurance regulators protect this vulnerable population against fraud. The grants were intended for a wide variety of senior investor protection efforts, such as hiring additional staff to investigate and prosecute cases, funding for new technology, equipment, and training for regulators, prosecutors, and law enforcement, and providing educational material to seniors to increase their awareness.

¹ The draft bill was posted in connection with the HFSC hearing entitled “Who is Standing Up for Consumers? A Semi-Annual Review of the Consumer Financial Protection Bureau” held on Oct. 16, 2019. See <https://financialservices.house.gov/calendar/eventsingle.aspx?EventID=404477>.

² 2016 Investor Protection Trust Elder Fraud Survey, http://www.investorprotection.org/downloads/IPT_EIFFE_Medical_Survey_News_Release_03-22-16.pdf.

³ See U.S. Senate Special Committee on Aging, *Fighting Fraud: Senate Aging Committee Identifies Top 10 Scams Targeting Our Nation's Seniors* 21 (2019).

CFA was among those voicing strong support for the program at the time.⁴ Unfortunately, in the nine years since the enactment of the Dodd-Frank Act, the CFPB has been unable to establish this important grant program due to uncertainty about the funding mechanism. The “Empowering States to Protect Seniors from Bad Actors Act” would clarify that the CFPB has both an obligation to establish and fund this grant program and the ability to fund it in the same manner as all of its other activities and responsibilities. Because the enactment of the bill and implementation of the 989(A) program will help prevent senior citizens from becoming victims of fraud, we urge you to work to ensure it is enacted.

We thank you for your attention to this important issue.

Respectfully submitted,



Barbara Roper
Director of Investor Protection

⁴ Letter from CFA, NASAA, AARP and Fund Democracy to Senate Banking Committee Chairman Christopher Dodd and Ranking Member Richard Shelby regarding the “Restoring American Financial Stability Act of 2009” Committee Print, Feb 2, 2010, <https://bit.ly/2QcVQq9>.

Letter of Support
Insured Retirement Institute (IRI)
Dec. 2, 2019



Insured Retirement Institute

1100 Vermont Avenue, NW | 10th Floor
Washington, DC 20005

t | 202.469.3000

f | 202.469.3030

www.IRionline.org

www.mylRionline.org

December 2, 2019

The Honorable Maxine Waters
Chairwoman
United States House of Representatives
Committee on Financial Services
2221 Rayburn House Office Building
Washington, DC 20515

The Honorable Patrick McHenry
Ranking Member
United States House of Representatives
Committee on Financial Services
2004 Rayburn House Office Building
Washington, DC 20515

Dear Representatives Waters and McHenry:

The Insured Retirement Institute (IRI)¹ writes to express our support for the enactment of the *Empowering States to Protect Seniors from Bad Actors Act*. The bill would amend the *Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank)* to provide clarification that senior investor protection grants made by the Consumer Financial Protection Bureau (CFPB) be made in the same manner as other grants issued by the Bureau.

The financial exploitation of senior citizens is a national imperative for Congress to address because it is costing and estimated \$2.9 billion to \$36.5 billion annually according to the Consumer Financial Protection Bureau [report](#) issued in February 2019. The [average loss per incident of financial exploitation is estimated to be \\$120,000](#), a figure which happens to align with the average amount of Americans have saved for retirement. As such, financial exploitation can erase a lifetime of savings and leave a retiree in financial ruin, compounding the retirement income crisis our nation is currently facing. With the population of older Americans expected to double in size to nearly 84 million citizens by 2050, there needs to be a concerted effort to combat financial exploitation.

Leading the fight to prevent and prosecute financial exploitation are the individual states' Adult Protective Services (APS) agencies. Unfortunately, APS offices across the country are underfunded, leaving them without the resources to fully investigate and prosecute financial exploitation. Section 989 (A) of the

¹ The Insured Retirement Institute (IRI) is the leading association for the entire supply chain of insured retirement strategies, including life insurers, asset managers, and distributors such as broker-dealers, banks and marketing organizations. IRI members account for more than 95 percent of annuity assets in the U.S., include the top 10 distributors of annuities ranked by assets under management, and are represented by financial professionals serving millions of Americans. IRI champions retirement security for all through leadership in advocacy, awareness, research, and the advancement of digital solutions within a collaborative industry community. Learn more at www.irionline.org.

Dodd-Frank directed the CFPB to establish grant programs to bolster efforts made by the individual states to protect vulnerable Americans. Unfortunately, while the CFPB was authorized to establish these grant programs, they have not been implemented due to alleged funding hindrances. The clarification to Section 989 (A) under the *Empowering States to Protect Seniors from Bad Actors Act* will improve protections for senior citizens by certifying that the CFPB is obligated to fund these programs.

The Insured Retirement Institute has a long history of advocating for the enactment of bipartisan, common-sense solutions that will help ensure that Americans can have a secure and dignified retirement. We believe these solutions include providing increased safeguards against bad actors looking to defraud individuals out of their savings. As Congress considers legislation to increase protections to deter and prevent the financial exploitation of senior citizens, we welcome the opportunity to work with you and your staff to advance the *Empowering States to Protect Seniors from Bad Actors Act*.

We thank you for your leadership in pursuing this legislation. If you have any questions, please do not hesitate to contact myself, Paul Richman, Chief Government and Political Affairs Officer at (202) 469-3004 or prichman@irionline.org, or John Jennings, Manager, Government Affairs at (202) 469-3017 or jjennings@irionline.org.

Sincerely,



Wayne Chopus
President & Chief Executive Officer
Insured Retirement Institute

Letter of Support
**National Council of Insurance
Legislators (NCOIL)**
Dec. 2, 2019

Atlantic Corporate Center
2317 Route 34, Suite 28
Manasquan, NJ 08726
732-201-4133
CHIEF EXECUTIVE OFFICER: Thomas B. Considine



PRESIDENT: Sen. Dan "Blade" Morrish, LA
VICE PRESIDENT: Rep. Matt Lehman, IN
TREASURER: Asm. Ken Cooley, CA
SECRETARY: Asm. Kevin Cahill, NY

IMMEDIATE PAST PRESIDENTS:
Sen. Jason Rapert, AR
Sen. Travis Holdman, IN

December 2, 2019

The Honorable Maxine Waters
Chairwoman
House Financial Services Committee
Washington D.C. 20515

The Honorable Patrick McHenry
Ranking Member
House Financial Services Committee
Washington D.C. 20515

Dear Chairwoman Waters and Ranking Member McHenry:

On behalf of the National Council of Insurance Legislators (NCOIL), I am writing in support of the draft legislation entitled "The Empowering States to Protect Seniors from Bad Actors Act." The legislation would amend Section 989(A) of the Dodd-Frank Act to clarify that senior investor protection grants made by the Consumer Financial Protection Bureau (CFPB) are funded in the same manner as other CFPB programs.

As you may know, NCOIL is a national legislative organization with the nation's 50 states as members, represented principally by legislators serving on their states' insurance and financial institutions committees. NCOIL writes Model Laws in healthcare, insurance and financial services, in accord with the State jurisdiction over insurance as established by the McCarran-Ferguson Act over seventy-four years ago, and to serve as an educational forum for public policy makers and interested parties. Founded in 1969, NCOIL works to assert the prerogative of legislators in making State policy when it comes to healthcare, insurance and financial services and educate State legislators on current and longstanding insurance and financial services issues.

Senior financial exploitation is a mounting problem across this country. Estimates indicate that 17 percent of Americans aged 65 or older – more than 6.8 million senior citizens – have been victims of financial exploitation, the form of which range from inappropriate investment recommendations, unreasonably high fees, or outright fraud.¹ According to the Government Accountability Office (GAO), seniors lose an estimated \$2.9 billion annually due to financial

¹ 2016 Investor Protection Trust Elder Fraud Survey:

http://www.investorprotection.org/downloads/IPT_EIFFE_Medical_Survey_Report_03-22-16.pdf



/NCOILorg

WEBSITE: www.ncoil.org



/NCOILorg

Sound Public Policy In 50 States For 50 Years

exploitation, although these numbers are likely substantially underreported.² Older Americans are particularly vulnerable to financial exploitation because financial decision-making ability can decrease with age, and they are often separated from family and other support networks at that point in their lives.

Section 989(A) of the Dodd-Frank Act authorizes the CFPB to make grants to states for the purpose of protecting seniors against financial exploitation. However, due to alleged funding impediments, the grant program has never been established. This legislation would remove those impediments to make clear that the CFPB has an both an ongoing obligation to establish and fund this grant program, and the ability to fund it in the same manner as all other CFPB programs.

Accordingly, NCOIL supports enactment of this legislation so that state legislators and other governmental authorities are provided with the appropriate resources to combat senior financial exploitation in a manner that meets the specific needs of each state.

Thank you and please do not hesitate to reach out if you wish to discuss this further. You can reach me at 732-201-4133 or at tconsidine@ncoil.org. Please also feel free to reach me on my cell at 732-245-0741.

With appreciation for your consideration, I am,

Very truly yours,



Thomas B. Considine
NCOIL CEO

² See U.S. Senate Special Committee on Aging, *Fighting Fraud: Senate Aging Committee Identifies Top 10 Scams Targeting Our Nation's Seniors*; pg. 21 (2019)

Letter of Support
Financial Services Institute (FSI)
Dec. 4, 2019



VIA ELECTRONIC MAIL

December 4, 2019

The Honorable Maxine Waters, Chairwoman
 The Honorable Patrick McHenry, Ranking Member
 U.S. House Committee on Financial Services
 2129 Rayburn House Office Building
 Washington, D.C. 20515

Re: The Empowering States to Protect Seniors from Bad Actors Act (Discussion Draft)

Dear Chairwoman Waters and Ranking Member McHenry:

On behalf of the Financial Services Institute¹ (FSI), I write to express support for the Empowering States to Protect Seniors from Bad Actors Act, which would amend Section 989(A) of the Dodd-Frank Act to specify that the Consumer Financial Protection Bureau's (CFPB) senior investor protection grant program be funded in the same manner as all other CFPB activities. FSI and its member firms are committed to the prevention of elder financial abuse and support efforts to prevent bad actors from using misleading designations.

The financial abuse of seniors is a growing concern nationally, particularly in light of the retirement savings crisis the country already faces. Combatting the financial abuse of seniors is critical to ensuring that this crisis does not worsen. Further, aging adults cannot afford to lose the valuable funds they rely on to ensure a secure retirement. Reports estimate that one in five Americans over the age of 65 has been victim to financial exploitation.² Financial advisors are often the first to notice the signs of possible financial abuse of senior clients and are best positioned to report it. Financial advisors need the tools and ability to share important information with the appropriate agencies that can assist the client.

In Section 989(A) of the Dodd-Frank Act, Congress directed the CFPB to establish a grant program to help states protect seniors from financial abuse. While the Dodd-Frank Act was passed in 2010, the grant program was not established due to alleged uncertainty about the funding mechanism. This legislation would clarify that the CFPB has an ongoing obligation to establish this program and the ability to fund it in the same manner as its other activities and programs.

¹ The Financial Services Institute (FSI) is an advocacy association comprised of members from the independent financial services industry, and is the only organization advocating solely on behalf of independent financial advisors and independent financial services firms. Since 2004, through advocacy, education and public awareness, FSI has been working to create a healthier regulatory environment for these members so they can provide affordable, objective financial advice to hard-working Main Street Americans.

² 2010 Investor Protection Trust Elder Fraud Survey, available at www.aging.senate.gov/imo/media/doc/SCA_Shaw_2_4_15.pdf

Thank you for considering FSI's comments. Should you have any questions, please contact our Director of Legislative Affairs, Hanna Laver, at (202) 499-7224.

Sincerely,

A handwritten signature in black ink, appearing to read "Dale Brown", written in a cursive style.

Dale E. Brown, CAE
President & CEO

Letter of Support
**American Council of Life Insurers (ACLI),
Association for Advanced Life
Underwriting (AALU),
Insured Retirement Institute (IRI),
and National Association of Insurance and
Financial Advisors (NAIFA)**
Dec. 4, 2019

December 4, 2019

The Honorable Maxine Waters
Chairwoman
House Committee on Financial Services
Washington, D.C. 20515

The Honorable Patrick McHenry
Ranking Member
House Committee on Financial Services
Washington, D.C. 20515

Dear Chairwoman Waters and Ranking Member McHenry:

ACLI, AALU, IRI and NAIFA¹ are writing to express our members' support for draft legislation titled, "The Empowering States to Protect Seniors from Bad Actors Act." This draft legislation would amend the Dodd-Frank Act to clarify that the senior investor protection grant program should be funded in the same manner as all other Consumer Financial Protection Bureau (CFPB) programs.

ACLI, AALU, IRI, and NAIFA and our companies are firmly committed to prohibiting abusive sales and marketing practices in our industry, particularly those targeting seniors. Given that the number of older adults continues to climb, elder financial abuse has become a problem in the United States. Unfortunately, bad actors target unsuspecting seniors due to isolation, vulnerability or deteriorating cognitive skills.

To help address this problem we were a strong supporter of the Senior Safe Act enacted in 2018. That law encourages better communication between financial services companies and regulatory agencies. The draft legislation is another step that will help states combat senior fraud.

Dodd-Frank Section 989(A) authorizes a grant program by the CFPB to assist states with protecting seniors against financial exploitation. Such a program will provide additional resources to state insurance departments and other state agencies to combat fraud against seniors. The state receiving such funds must have implemented rules that conform to minimum requirements set forth by the National Association of Insurance Commissioners (NAIC) and the North American Securities Administrators (NASAA).

While the program was initially authorized in 2010 as part of the Dodd-Frank Act, it was never established, ostensibly due to certain alleged funding impediments. This legislation will remove those impediments and make clear that the CFPB has an ongoing obligation to establish and fund these grants.

Thank you for your attention to this important issue and for the opportunity to voice our support for this bill. We look forward to working with you to move the legislative process forward.

Sincerely,

Susan K. Neely
ACLI President and CEO

Marc Cadin
AALU President and CEO

Wayne Chopus
IRI President and CEO

Kevin M. Mayeux, CAE
NAIFA CEO

¹ The American Council of Life Insurers (ACLI) advocates on behalf of 280 member companies dedicated to providing products and services that promote consumers' financial and retirement security. 90 million American families depend on our members for life insurance, annuities, retirement plans, long-term care insurance, disability income insurance, reinsurance, dental and vision and other supplemental benefits. ACLI represents member companies in state, federal and international forums for public policy that supports the industry marketplace and the families that rely on life insurers' products for peace of mind. ACLI members represent 95 percent of industry assets in the United States.

AALU is the leading organization of financial professional who provide life insurance and retirement planning solutions for individual, families, and businesses. AALU has a rich history of success with a single focus on the issues impacting life and annuity products, and the clients its members serve. Headquartered in Washington, D.C., AALU is committed to providing its members with the essential tools and services required to help grow their businesses, serve their clients, and protect the financial and retirement security of the American people.

The Insured Retirement Institute (IRI) is the leading association for retirement income industry and only association representing the entire supply chain of insured retirement strategies. Our mission is to advocate for sustainable retirement solutions Americans need to help achieve a secure and dignified retirement; provide consumer education and outreach efforts to promote the value of retirement income planning; and raise consumer knowledge of retirement income strategies through public engagement campaigns. Our members include major insurers, asset managers, broker-dealers/distributors, banks, solution providers and more than 150,000 financial professionals. Our member companies account for more than 95% of annuity assets in the United States and include the top 10 distributors of annuities ranked by assets under management.

Founded in 1890, the National Association of Insurance and Financial Advisors (NAIFA) is the oldest, largest and most prestigious association representing the interests of insurance professionals from every congressional district in the United States. NAIFA members assist consumers by focusing their practices on one or more of the following: life insurance and annuities, health insurance and employee benefits, retirement planning, multiline, and financial advising and investments. NAIFA's mission is to advocate for a positive legislative and regulatory environment, enhance business and professional skills, and promote the ethical conduct of its members.

Letter of Support
Financial Planning Coalition
Dec. 18, 2019



December 18, 2019

The Honorable Maxine Waters
Chairwoman
House Committee on Financial Services
Washington, D.C. 20515

The Honorable Patrick McHenry
Ranking Member
House Committee on Financial Services
Washington, D.C. 20515

RE: Support for "*The Empowering States to Protect Seniors from Bad Actors Act*"
(Discussion Draft)

Dear Chairwoman Waters and Ranking Member McHenry:

On behalf of the Financial Planning Coalition,¹ we are writing to express support for the draft legislation entitled "The Empowering States to Protect Seniors from Bad Actors Act," which would enhance the ability of state regulators to protect seniors from financial exploitation. It would achieve this by clarifying that the senior investor protection grant program authorized by Congress in Section 989(A) of the Dodd-Frank Act to be administered by the Consumer Financial Protection Bureau (CFPB) may be funded in the same manner as all other activities of the agency.

Senior financial exploitation is an urgent and growing problem across the country. Although it is considered to be an underreported crime, financial exploitation is increasingly affecting aging adults, particularly those with cognitive impairments. These crimes are now so widespread that elder financial abuse often is called the "crime of the twenty-first century." Studies show that financial exploitation is the most common form of elder abuse, with estimates of annual losses to older adults ranging from \$2.9 billion to \$36.5 billion.²

The more than 86,000 CFP® professionals who are stakeholders and members of the Coalition organizations see first-hand the damage that occurs when seniors are the victims of financial scams. Senior financial exploitation is particularly pernicious since the victims often are past the point in their earning years where they can recover the losses. This problem is

¹ Comprised of Certified Financial Planner Board of Standards ("CFP Board"), the Financial Planning Association® ("FPA"), and the National Association of Personal Financial Advisors ("NAPFA"), the Financial Planning Coalition is a collaboration of the leading national organizations representing the development and advancement of the financial planning profession. Together, the Coalition seeks to educate policymakers about the financial planning profession, to advocate for policy measures that ensure financial planning services are delivered in the best interests of the public, and to enable the public to identify trustworthy financial advisers. See, <http://financialplanningcoalition.com>

² *Suspicious Activity Reports on Elder Financial Exploitation: Issues and Trends*, CFPB Office of Financial Protection for Older Americans (February 2019).
https://files.consumerfinance.gov/f/documents/cfpb_suspicious-activity-reports-elder-financial-exploitation_report.pdf

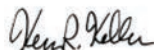
expected to intensify with the aging of the baby boom generation and the increases in average life expectancy.

State regulators are the first line of defense in the fight against senior financial exploitation. In recognition of the role they play, Section 989(A) of the Dodd-Frank Act established a grant program within the CFPB designed to help state securities and insurance regulators protect this vulnerable population against fraud. The grants were intended to be used for a variety of senior investor protection efforts, including hiring additional staff to investigate and prosecute cases; funding new technology, equipment and training for regulators, prosecutors and law enforcement; and providing educational material to seniors to increase their awareness.

The CFPB has not established this important grant program in the nine years since the enactment of the Dodd-Frank Act because of uncertainty around the funding mechanism. The "Empowering States to Protect Seniors from Bad Actors Act" would clarify that the CFPB has both an obligation to establish and fund this grant program and the ability to fund it in the same manner as all its other activities and responsibilities. Enactment of this legislation and implementation of the Section 989(A) grant program will help prevent older Americans from becoming victims of fraud. We urge you to support the legislation and ensure it is enacted.

Please contact Maureen Thompson, vice president of policy, CFP Board of Standards, at (202) 379-2281 or mthompson@cfpboard.org if you have questions or need additional information.

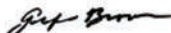
Sincerely,



Kevin R. Keller, CAE
Chief Executive Officer
CFP Board



Lauren Schadle, CAE
Executive Director/CEO
FPA®



Geoffrey Brown, CAE
Chief Executive Officer
NAPFA



June 16, 2020

The Honorable Maxine Waters
Chairwoman
Committee on Financial Services
U.S. House of Representatives
Washington, DC 20515

The Honorable Patrick McHenry
Ranking Member
Committee on Financial Services
U.S. House of Representatives
Washington, DC 20515

Dear Chairwoman Waters and Ranking Member McHenry:

The American Securities Association (ASA)¹ commends the Subcommittee on National Security, International Development, and Monetary policy for holding today's hearing entitled "Cybercriminals and Fraudsters: How Bad Actors are Exploiting the Financial System During the COVID-19 Pandemic." The hearing comes at a critical time and should highlight some of the serious risks posed to investors and savers by cybercriminals, particularly nation state actors such as China.

The ASA believes the largest cyberthreat currently facing the U.S. financial system is the pending collection of the personal and financial information (PII) of *every* American investor by the Securities and Exchange Commission's (SEC) Consolidated Audit Trail database (CAT). Despite the CAT becoming an obvious "one-stop-shop" for cybercriminals to steal the identities of Americans or manipulate our equity markets, the SEC has decided to march forward with the collection of retail investor PII.

This comes at a time when the coronavirus pandemic has only exacerbated the cyber threat against government institutions and the financial industry. According to [recent report](#) from a leading cybersecurity firm, "from the beginning of February to the end of April 2020, attacks targeting the financial sector have grown by 238%." By moving forward now, the SEC will put the PII of millions of America's mom-and-pop investors at risk while marginally improving the SEC's ability to oversee the U.S. stock market.

The CAT will undoubtedly become a top target for hackers supported by the Chinese government, who have already been behind hacks on the Office of Personnel Management, National Aeronautics and Space Administration, National Security Agency, as well as countless other government and private entities in recent years. Even the SEC was hacked in 2016—a

¹ The ASA is a trade association that represents the retail and institutional capital markets interests of regional financial services firms who provide Main Street businesses with access to capital and advise hardworking Americans how to create and preserve wealth. The ASA's mission is to promote trust and confidence among investors, facilitate capital formation, and support efficient and competitively balanced capital markets. This mission advances financial independence, stimulates job creation, and increases prosperity. The ASA has a geographically diverse membership base that spans the Heartland, Southwest, Southeast, Atlantic, and Pacific Northwest regions of the United States.



American Securities Association
1455 Pennsylvania Ave. NW, Suite 400
Washington, D.C. 20004



AmericanSecurities.org
@amersecurities



202.621.1784



breach it didn't discover until August 2017. Recent reports also describe Chinese efforts to hack the email accounts of Presidential [campaigns](#) and to steal information related to development of a [coronavirus vaccine](#). The ASA has been warning of the CAT's national security risk since last year and published an op-ed in *The Hill* entitled "The National Security Risk No One Is Talking About" (Exhibit A). China remains one of the top threats to consumer privacy and national security, and by centralizing all this information in the CAT, we are giving them a target too big to ignore.

Given the threats to the financial and personal security posed by the CAT, the ASA recently filed a lawsuit against the SEC to prohibit the collection of retail investor PII. We first announced the lawsuit in a *Wall Street Journal* op-ed (Exhibit B). The ASA also launched MyDataMyVote.com, a nationwide grassroots movement to give a voice to every American investor that is concerned about their personal privacy and does not want their information stored in a centralized, unsecure government database. The ASA will continue to fight on behalf of American investors and put an end to this misguided effort by the SEC.

We are calling on you to stop the SEC from continuing down this perilous path and to protect the private information of every American retail investor. We appreciate the Subcommittee's attention to this important issue and look forward to assisting in any way that we can.

Sincerely,

Christopher A. Iacovella

Christopher A. Iacovella
Chief Executive Officer
American Securities Association



American Securities Association
1455 Pennsylvania Ave. NW, Suite 400
Washington, D.C. 20004



AmericanSecurities.org
@amersecurities



202.621.1784



Exhibit A


The national security risk no one is talking about

BY CHRISTOPHER A. IACOVELLA, OPINION CONTRIBUTOR — 07/03/19 08:30 AM EDT

Today's security threats continue to evolve as foreign adversaries and cyber criminals work tirelessly to influence U.S. elections, target and breach our country's largest companies, and steal the sensitive personal information of the American people.

The government's responsibility to protect us from external threats is as important today as it's ever been. President Trump's national security strategy reaffirms this guiding principle by stating "[o]ur government's first duty is to its people, to our citizens — to serve their needs, to ensure their safety, to preserve their rights, and to defend their values."

Policymakers in Washington are modernizing our national security defenses to address today's growing threats. But a little-known government data collection initiative at the U.S. Securities and Exchange Commission (SEC) threatens to undermine these efforts by creating a target-rich environment for cyber criminals and state actors, such as China, to steal the personally identifiable information (PII) of every American who has money in the stock market. PII includes your name, address, date of birth and financial account information.

After the 2010 stock market "Flash Crash," the SEC required broker-dealers, trading venues and stock exchanges to report all stock trades and customer information to a single database, known as the Consolidated Audit Trail (CAT). While the SEC argues this expansive new database would allow it to analyze market events quicker, it never considered the national security risks of storing the PII of every American investor in a central location.

Preventing fraud and manipulation in our markets is very important, and we don't oppose the creation of the CAT to achieve these goals. We do, however, believe this can be done without collecting the PII of every American investor and serving it up to America's adversaries in a single all-you-can-steal database.



American Securities Association
1455 Pennsylvania Ave. NW, Suite 400
Washington, D.C. 20004



AmericanSecurities.org
@amersecurities



202.621.1784


american securities association
America's Voice for Main Street's Investors

Our concern is justified by the numerous high-profile cyber-attacks at corporations and government agencies across the U.S. Even the National Security Agency was hacked when Chinese agents stole NSA cyber tools so they could re-deploy them against U.S. targets.

A recent U.S. Intelligence Community "Worldwide Threat Assessment" report warned that "[o]ur adversaries and strategic competitors will increasingly use cyber capabilities – including cyber espionage, attack and influence – to seek political, economic, and military advantage over the United States." The report concludes that adversaries, including China, will "increasingly use cyber operations to threaten both minds and machines in an expanding number of ways—to steal information, to influence our citizens, or to disrupt critical infrastructure."

Secretary of State Pompeo also warned that the Chinese are using cyberattacks to obtain information on susceptible Americans in order to recruit them as double agents. When foreign adversaries openly use this kind of warfare to advance their political agenda, the U.S. government must do everything in its power to protect its citizens from the threat they pose.

Leaders on both sides of the aisle, including Sens. Chuck Schumer (D-N.Y.) and Marco Rubio (R-Fla.), believe China is playing a zero-sum game and willing to win at all costs. FBI Director Wray put a fine point on that belief, saying China is "determined to steal its way up the economic ladder at our expense." Hacking into the CAT may represent an opportunity that is too good to pass up.

The SEC has been hacked before, and it knows the CAT will put the PII of millions of American investors at risk. The Chairman said "[w]e expect we will face the risk of unauthorized access to the CAT's central repository and through such access, intruders could potentially obtain, expose and profit from the trading activity and PII of investors and other market participants." This disclaimer is pointless to the millions of Americans who could have their identity stolen and their lives ruined.

From the halls of Congress to our nation's highest law enforcement and intelligence agencies, it's clear the cyber threat China poses to America cannot be ignored. It's time for the SEC to do the right thing.

American savers and retirees across the country and across party lines overwhelmingly agree that now is the time for leaders in Washington to stop this misguided course of action. The agency can protect American investors and maintain confidence in our capital markets without creating a one-stop-shop for cyber criminals that risks our national security.

Christopher A. Iacovella is the chief executive officer of the American Securities Association.



American Securities Association
1455 Pennsylvania Ave, NW, Suite 400
Washington, D.C. 20004



AmericanSecurities.org
@amersecurities



202.621.1784



Exhibit B

THE WALL STREET JOURNAL.

Why We're Suing the SEC

In the name of speeding up its work, the agency is putting individual investors at risk of identity theft.

By Christopher A. Iacovella
May 17, 2020 2:43 pm ET

Mom-and-pop investors didn't cause the 2010 market blip known as the "flash crash," but the Securities and Exchange Commission is suggesting as much to justify a new government program that will collect and store the most sensitive personal information of every U.S. retail investor in a single database. This exposes investors to a high risk of identity theft. That's why the American Securities Association, which I lead, is suing the commission.

We supported the SEC's 2012 creation of the Consolidated Audit Trail (CAT) database to keep track of institutional investors. But collecting sensitive personal and financial information—including address, birth year and transaction data—from retail investors has always been a solution in search of a problem. Regulators struggled to pinpoint the cause of the 2010 drop, and the CAT arose as a surveillance tool to save the SEC time in future detective work.

The commission claims it needs the data to prosecute insider trading. Yet the SEC has no trouble doing that now. Between 2011 and 2019, the SEC's Division of Enforcement brought more than 400 cases against individuals accused of violating insider trading rules. More data may make the job easier, but, in our view, invading the privacy of every small investor and exposing them to the risk of identity theft isn't worth that marginal gain.

Our organization hoped the SEC would change course, but the new database has left us with a choice: expose our customers to identity theft or protect their right to privacy. We choose the latter. On Monday the American Securities Association will file a lawsuit against the SEC. We take no pleasure in suing our regulator, and we didn't come to this decision lightly. But the industry can't abide a privacy threat to every U.S. investor. Saving and investing for retirement is hard enough. Americans shouldn't also have to worry about cybercriminals from China and Russia.

Defense and intelligence agencies routinely warn that U.S. adversaries and bad actors across the globe are targeting individual Americans to steal their identities. Earlier this year a federal grand jury [indicted](#) four members of the Chinese People's Liberation Army for stealing the personal financial data of nearly half the American population in the [Equifax](#) breach. Similar high-profile



American Securities Association
1455 Pennsylvania Ave. NW, Suite 400
Washington, D.C. 20004



AmericanSecurities.org
[@amersecurities](#)



202.621.1784



american securities association

America's Voice for Main Street's Investors

hacks compelled U.S. intelligence officials to warn the public in December 2018 that the Chinese are using cyberattacks to obtain information on susceptible Americans to try to recruit them as spies.

Former FBI Director James Comey issued a warning in 2014 that should worry every American: "There are two kinds of big companies in the United States. There are those who've been hacked by the Chinese and those who don't know they've been hacked by the Chinese." His words, not ours.

The SEC is not impregnable. It was hacked in 2016—a breach it didn't discover until August 2017. SEC Chairman Jay Clayton [warned](#) in September 2017 after the breach that "we will face the risk of unauthorized access to the CAT's central repository and other efforts to obtain sensitive CAT data. Through such access, intruders could potentially obtain, expose and profit from the trading activity and personally identifiable information of investors." Despite these warnings, the SEC seems committed to collecting the personal information of everyday American investors. Only in Washington could the creation of a one-stop shop for cyberhackers seem like a good idea.

The SEC is compelling us to send the data of every individual U.S. investor to an unsecure database. We're filing this lawsuit to stand up for investors, to maintain trust and confidence in America's equity markets, and to force the SEC to publicly defend this dangerous policy.

Mr. Iacovella is CEO of the American Securities Association.



American Securities Association
1455 Pennsylvania Ave. NW, Suite 400
Washington, D.C. 20004



AmericanSecurities.org
[@amersecurities](#)



202.621.1784



June 16, 2020

The Honorable Emanuel Cleaver
Chairman
Subcommittee on National Security, International Development and Monetary Policy
House Committee on Financial Services
Washington, DC 20515

The Honorable French Hill
Ranking Member
Subcommittee on National Security, International Development and Monetary Policy
House Committee on Financial Services
Washington, DC 20515

Dear Chairman Cleaver and Ranking Member Hill:

On behalf of the members of the Consumer First Coalition (CFC), I am pleased to submit this statement for the record for your hearing titled "Cybercriminals and Fraudsters: How Bad Actors are Exploiting the Financial System During the COVID-19 Pandemic." CFC represents a group of leading financial services companies committed to combating new forms of fraud, protecting identities, and upholding the privacy protections that are a hallmark of the financial services industry. To meet these objectives and ensure consumer data and accounts are kept safe, the financial sector is constantly evolving and adapting to meet the dynamic challenges posed by sophisticated cyber criminals.

The COVID-19 pandemic presents bad actors with tremendous opportunities to commit fraud, with criminals focusing their efforts on targeting the billions of dollars moving through the banking and payments system. For example, according to the Identity Theft Resource Center, scammers are adapting their tactics using calls, texts and social media to phish for consumers' sensitive financial information with fraudulent pandemic-related themes.¹ In addition, the Federal Trade Commission reported that from January through April of this year it received 18,235 reports related to COVID-19, with consumers reporting losses of \$13.44 million to fraud.²

Federal financial authorities have also taken steps to alert financial institutions of the spike in financial scams associated with COVID-19. For example, the Consumer Financial Protection Bureau (CFPB) and Federal Deposit Insurance Corporation (FDIC) each published alerts warning consumers to be mindful of pandemic-related scams. The FDIC even noted the emergence of scams in which imposters pretend to be officials of the agency in an effort to carry out fraudulent schemes.³

¹ See "COVID-19-related Scams on the Rise," accessed at <https://www.cbs17.com/news/covid-19-related-scams-on-the-rise/>

² "Covid-19 Scam Reports, by the Numbers." Federal Trade Commission. Accessed at <https://www.consumer.ftc.gov/blog/2020/04/covid-19-scam-reports-numbers>

³ See "Beware of Scams Related to the Coronavirus" and "FDIC: Insured Bank Deposits are Safe; Beware of Potential Scams Using the Agency's Name," accessed at <https://www.consumerfinance.gov/about-us/blog/beware-coronavirus-related-scams/> and <https://www.fdic.gov/news/news/press/2020/pr20032.html>.



In addition, FINRA alerted broker-dealers to a rise in reports of fraudulent account openings and money transfers. In particular, the agency noted how criminals are using synthetic identities to establish new brokerage accounts, funding these accounts by using stolen bank account data to transfer funds from consumers' checking accounts, and then quickly accessing the funds through ATM withdrawals or even linking to a third-party bank account for exfiltration.⁴

Synthetic identity fraud combines stolen Social Security numbers (SSNs) with fabricated personal information to create a synthetic credit history. This is especially problematic for children because they are less likely to have their SSN associated with an established credit history. Once established, the fraudulent credit history is utilized to apply for credit products or, as FINRA points out, establish brokerage accounts. Children whose SSN has been compromised today through synthetic identity fraud will likely not become aware of it for many years, perhaps when they apply for a college loan or to open their first bank account.

In 2018, Congress enacted Section 215 of S. 2155, the Economic Growth, Regulatory Relief, and Consumer Protection Act. This law directs the Social Security Administration (SSA) to build a system to provide the financial industry the ability to verify whether a given name, date-of-birth and SSN match with what the SSA has on file. As part of a financial institution's underwriting and fraud review of a new applicant, this piece of information can help prevent synthetic identities from getting off the ground and harming the consumers whose SSNs were compromised.

Within the next month, a pilot of this new system – called the Electronic Consent Based SSN Verification System, or eCBSV – is set to launch. CFC has been working closely with SSA and other industry partners to ensure implementation meets Congressional expectations for a sophisticated system that will help protect consumers. While broad adoption and use of eCBSV across the financial industry is many months away, this effort is a strong example of how the best solutions to meeting the evolving cyber threat landscape often requires close collaboration among public and private stakeholders.

In conclusion, thank you for holding this hearing today. While developing the eCBSV is not a panacea, it will provide a key tool to help protect millions of Americans who might otherwise become victims of synthetic identity fraud. CFC is committed to working with policymakers to address the new and expanding fraud threats facing consumers that have only been exacerbated by this recent pandemic.

Sincerely,

/s/

Jason Kratovil
Executive Director

⁴ FINRA Regulatory Notice 20-13, "FINRA Reminds Firms to Beware of Fraud During the Coronavirus (COVID-19) Pandemic." Accessed at <https://www.finra.org/rules-guidance/notices/20-13>

QFR Responses of Jamil N. Jaffer¹
on
Cybercriminals and Fraudsters: How Bad Actors Are Exploiting
the Financial System During the COVID-19 Pandemic
before the
Subcommittee on National Security, International Development and Monetary Policy
of the
United States House of Representatives Committee on Financial Services

June 16, 2020

Rep. French Hill

Questions for Jamil Jaffer

1. During your testimony, you discussed at length the success of the European Systemic Risk Board (ESRB). Is there companion entity in the United States? If so, what is it?

Thank you for the question, Ranking Member Hill. As you may know, the European Systemic Risk Board is “responsible for the macroprudential oversight of the EU financial system and the prevention and mitigation of systemic risk...[and] therefore has a broad remit, covering banks, insurers, asset managers, shadow banks, financial market infrastructures and other financial institutions and markets.”² In addition, “[i]n pursuit of its macroprudential mandate, the ESRB monitors and assesses systemic risks and, where appropriate, issues warnings and recommendations.”³

While there is no exact parallel in the United States, at least two entities have similar or related functions. For example, the Financial Stability Oversight Council (FSOC) of the U.S. Department of Treasury is “charged with identifying risks to the financial stability of the United States; promoting market discipline; and responding to emerging risks to the stability of the

¹ Jamil N. Jaffer currently serves as Founder & Executive Director of the National Security Institute and as an Assistant Professor of Law and Director, National Security Law & Policy Program at the Antonin Scalia Law School at George Mason University and is affiliated with Stanford University’s Center for International Security and Cooperation. Mr. Jaffer also serves as Senior Vice President for Strategy, Partnerships & Corporate Development at IronNet Cybersecurity, a startup technology products company headquartered in the Washington, DC metropolitan area. Among other things, Mr. Jaffer previously served as Chief Counsel & Senior Advisor to the Senate Foreign Relations Committee, Senior Counsel to the House Intelligence Committee, Associate Counsel to President George W. Bush, and Counsel to the Assistant Attorney General for National Security in the U.S. Department of Justice. Mr. Jaffer provides these responses to the Committee in his personal and individual capacity and not on behalf of any organization or entity, including but not limited to any current or former employer.

² See European Systemic Risk Board, *Mission and Establishment*, available online at <https://www.esrb.europa.eu/about/background/html/index.en.html>.

³ *Id.*

United States' financial system.”⁴ The FSOC has ten voting members and five nonvoting members and “brings together the expertise of federal financial regulators, state regulators, and an independent insurance expert appointed by the President.”⁵ According to the Department of Treasury, the FSOC is authorized to, among other things, facilitate regulatory coordination and information sharing and collection and to designate certain systemic entities for additional supervision and oversight.⁶ In addition, in order to “help with the identification of emerging risks to financial stability, the FSOC can provide direction to, and request data and analyses from, the newly created Office of Financial Research (OFR) housed within Treasury.”⁷

Similarly, the Federal Reserve, among other things, “promotes the stability of the financial system and seeks to minimize and contain systemic risks through active monitoring and engagement in the U.S. and abroad...[and] promotes the safety and soundness of individual financial institutions and monitors their impact on the financial system as a whole.”⁸ As part of these efforts, the Fed supervises “systemically important financial institutions (SIFIs) including large bank holding companies (BHCs), the U.S. operations of certain foreign banking organizations (FBOs), and financial market utilities (FMUs)”⁹ and also “serves as a ‘consolidated supervisor’ of nonbank financial companies that the FSOC has determined should be supervised by the Federal Reserve Board and subject to prudential standards.”¹⁰ In addition, the Fed “actively monitors indicators of the riskiness of SIFIs...to help identify vulnerabilities” and “imposes certain regulatory requirements on SIFIs in order to limit potentially risky activities by these institutions and to mitigate spillover of distress into the broader economy.”¹¹ The Fed notes that “[o]ne important element of enhanced supervision of SIFIs is the stress-testing process...[which] includes macroprudential elements such as examination of the loss-absorbing capacity of institutions...conducting horizontal testing...to understand [] potential correlated exposures; and consideration of the effects of counterparty distress on the largest, most interconnected firms.”¹²

⁴ See U.S. Department of Treasury, *Financial Stability Oversight Council*, available online at <<https://home.treasury.gov/policy-issues/financial-markets-financial-institutions-and-fiscal-service/fsoc>>.

⁵ *Id.*

⁶ See U.S. Department of Treasury, *About FSOC*, available online at <<https://home.treasury.gov/policy-issues/financial-markets-financial-institutions-and-fiscal-service/fsoc/about-fsoc>>.

⁷ *Id.*

⁸ See The Federal Reserve, *About the Federal Reserve System*, available online at <<https://www.federalreserve.gov/aboutthefed/structure-federal-reserve-system.htm>>.

⁹ See The Federal Reserve, *THE FEDERAL RESERVE SYSTEM PURPOSES & FUNCTIONS* 65 (10th ed. 2016), available online at <https://www.federalreserve.gov/aboutthefed/files/pf_complete.pdf>.

¹⁰ *Id.* at 65-66.

¹¹ *Id.* at 66.

¹² *Id.* at 66-67.

2. Can the role of the Pittsburgh-based cyber fusion center expand? What are its successes? Limitations?

Again, thank you for the question, Ranking Member Hill. As you know, according to the FBI, the National Cyber-Forensics & Training Alliance (NCFTA), a nonprofit based in Pittsburgh that was established over two decades ago, has “become an international model for bringing together law enforcement, private industry, and academia to share information to stop emerging cyber threats and mitigate existing ones.”¹³ Per the FBI, NCFTA “essentially works as an early-warning system” by taking advantage of staff assigned by alliance members to the NCFTA as well as agents and analysts assigned to the FBI’s the Cyber Initiative and Resource Fusion Unit (CIRFU) which is attached to the NCFTA, Carnegie Mellon University’s Computer Emergency Response Team (CERT), and the FBI’s Internet Crime Complaint Center (IC3).¹⁴ The information shared through NCFTA and CIRFU, including with global partners, has led to a number of major takedowns, including the disruption of the Dark Market website and operations related to the Coreflood and Zeus malware used for cyber financial exploitation.¹⁵

As with all such successful organizations, the more resources and authorities—public and private alike—that can be provided could potentially enable more effective operations, if employed in an appropriate and judicious manner. Moreover, to the extent that such organizations are able to build out an effective collective defense capability—moving to sharing real-time, full-scale, actionable threat intelligence and engaging collective defensive action—across the public-private divide as well as across multiple industry segments—the more successful they will be at addressing the current imbalance between attackers and defenders,¹⁶ particularly when we are talking about the type of nation-state and sophisticated criminal adversaries targeting our financial institutions.

¹³ See Federal Bureau of Investigation, *The NCFTA: Combining Forces to Fight Cyber Crime* (Sept. 16, 2011), available online at <<https://www.fbi.gov/news/stories/the-ncfta-combining-forces-to-fight-cyber-crime>>.

¹⁴ *Id.*

¹⁵ *Id.*

¹⁶ See GEN (ret.) Keith B. Alexander & Jamil N. Jaffer, *The Other Crisis: U.S. Companies Still Need Help Against Cyberattacks*, *Barron's* (Mar. 16, 2020), available online at <<https://www.barrons.com/articles/cyberspace-solarium-commission-urges-collective-defense-51584364449>>.

Questions for the Record

Hearing: "Cybercriminals and Fraudsters: How Bad Actors Are Exploiting the Financial System During the COVID-19 Pandemic"
 Subcommittee on National Security, International Development, and Monetary Policy
 (Committee on Financial Services)
 June 16, 2019

Chairman Perlmutter

1. In your written testimony, you recommend creating a tax incentive for "financial sector companies that dedicate at least 10 percent of their IT budgets towards cybersecurity" and comply with the NIST Cyber Security Framework. In determining compliance with the NIST framework under your proposal, who would be a suitable third-party validator to ensure a firm is complying with NIST?

VMware response: *The major professional services firms like Booz Allen, Kroll, Optiv, E&Y, & Deloitte would all be capable of providing third-party validation. These firms all have cyber practices and would have experience in dealing with NIST.*

Rep. French Hill

What specific internal and external IT exam practices should be added to in the annual bank exam process? What specific internal and external IT exam practices should be added to in the annual bank exam process?

VMware response: *We recommend the following new tests or questions be added to the annual bank process current process:*

Internal controls:

1. ***Has the financial institution integrated all the information security controls?***
Specifically, cross platform integrations like the network and end point security controls are interconnected.
2. ***Does the financial institution have the ability to audit current system state?*** *Essentially, does the bank have the ability to actively look at every endpoint to see if every system/application on the network is up to date and configured correctly.*
3. ***Does the financial institution have a threat hunting team and do they conduct threat hunts on a monthly basis?*** *Currently most cybercriminals live in a network for weeks without detection. This would require banks to actively look for cyber attackers.*

4. ***Does the financial institution implement micro segmentation?*** *Micro segmentation is a network security technology that enables security architects to divide a data center or network into distinct security segments at the workload level. This is typically done in software and enables the architect to deploy flexible security policies deep inside a data center (using software) instead of installing multiple physical firewalls. This stops cyber-attacks from moving laterally internally across a data center once a hacker has breached the external perimeter.*
5. ***Does the financial institution apply application control?*** *This refers to white listing which is monitoring an application to ensure it is doing the exact thing it has been created to do, checking it for behavioral anomalies and then suppressing them.*
6. ***Can the financial institution apply just in time administration?*** *Just in time administration means that no IT administrator has perpetual credentials and limits the amount of time an administrator has access to privileged account management for an organization. This limits the threat surface of a financial institution.*

External contracts:

1. ***Are you conducting cyber threatening hunting in your Managed Service Provider?*** *This refers to whether or not an institution is actively searching their network for cyber intrusions. Alternatively, the managed service provider could share the results of their cyber threat hunting on a regular basis.*

