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 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 enhanced 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 Investigations
- 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 dangerous of inadequately securing their systems, devices and information.