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.