Prepared Statement of Jamil N. Jaffer[1]
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/bill/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 globe[18] 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 Jermy 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 it 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/strategiceurope/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 200,0000 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 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/>.