MAXINE WATERS, CA
CHAIRWOMAN

United States House of Representatives
Committee on Financial Services
2129 Rayburn House Office Building
Washington, D.C. 20515

PATRICK MCHENRY, NC
RANKING MEMBER

June 11, 2020

Memorandum

To: Members, Committee on Financial Services
From: FSC Majority Staff
Subject: June 16, 2020, "Cybercriminals and Fraudsters: How Bad Actors Are Exploiting the Financial System During the COVID-19 Pandemic"

The Subcommittee on National Security, International Development and Monetary Policy will hold a virtual hearing entitled, "Cybercriminals and Fraudsters: How Bad Actors Are Exploiting the Financial System During the COVID-19 Pandemic," on Tuesday, June 16, 2020, at 12:00 p.m., on the virtual meeting platform Cisco Webex. This single-panel hearing will have the following witnesses:

- **Mr. Tom Kellermann,** Head of Cybersecurity Strategy, VMware
- **Mr. Kelvin Coleman,** Executive Director, National Cyber Security Alliance
- **Ms. Amanda W. Senn,** Chief Deputy Director, Alabama Securities Commission; on behalf of the North American Securities Administrators Association (NASAA)
- **Mr. Jamil Jaffer,** Founder & Executive Director, National Security Institute, Assistant Professor of Law & Director, National Security Law & Policy Program

Overview

According to the Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3), "the number of cybersecurity complaints to the IC3 in the last four months has spiked from 1,000 daily before the pandemic to as many as 4,000 incidents in a day."[1] These reports in the first four months of the COVID-19 pandemic are near the total reported amount of 2019 complaints.[2]

The financial services sector is also under increased duress due to COVID-19 related cyber-criminal activity. A May 2020 survey of financial institutions (FIs) found that 80% of surveyed banks report a year-on-year increase in cyberattacks against the sector surging 238% during the COVID-19 crisis (February-April 2020).[3] The volume of attacks, as reported by many of the largest FIs, moved across the globe towards the U.S. in line with the movement of the virus and has continued to ebb and flow with the undulations of the COVID-19 news cycle.[4]

These cyber vulnerabilities are exacerbated by the unusually large numbers of employees in the United States working remotely.[5] According to the National Cyber Security Alliance (NCSA), "basic security measures need to be taken to protect the individual and enterprise from cyber criminals who are taking advantage of lax telework security practices."[6] The technology to support remote work – such as Virtual

[1] The Hill, FBI sees spike in cyber crime reports during coronavirus pandemic, Maggie Miller, Apr 16, 2020
[2] FBI: Internet Crime Complaint Center (IC3) website, 2019 Internet Crime Report
[3] VMware Carbon Black, Modern Bank Heists 3.0 Tom Kellermann, R. Murphy, May 2020
[4] Ibid.
[5] Gallup, Reviewing Remote Work in the U.S. Under COVID-19, Adam Hickman, Ph.D., Lydia Saad. May 22, 2020
[6] National Cyber Security Alliance, NCSA website, Security Tips for Remote Workers

Private Networks, DNS routers, cloud deployments, and videoconferencing platforms – has the potential to introduce new points of exploitable weakness for opportunistic cybercriminals. Strains on IT and cybersecurity staff as a result of illness or stay-at-home orders can result in slower updates to software and maintenance to systems. Further, poor home-based digital hygiene (e.g., weak passwords on personal computers, poorly secured home Wi-Fi routers, and family linking internet-connected devices) increases the possibility that an employee might unintentionally pass a computer virus to a company's main system.[7]

Many persons in the United States have already been victims of cyber breaches, whether leaked directly or through other parties.[8] As a result, their personally identifiable information (PII), such as social security numbers and dates of birth, is already available for purchase on the dark web.[9] Criminals, often through shell companies[10], can use this PII to apply for state and federal benefits and to perpetrate other types of fraud. Synthetic identification, where the entire "person" is fake, but built over time by criminals combining fake information with real, verifiable PII[11], is also used increasingly to exploit the financial services sector[12]. This hard-to-detect fraud has, in 2018 alone, directly impacted 14.4 million consumers and resulted in losses of approximately $14.7 billion.[13]

Methods Used by Cyber Criminals to Target Victims

According to the Financial Crimes Enforcement Network (FinCEN), cyber criminals are utilizing traditional attack strategies, and modifying or increasing them to exploit the unique challenges and anxieties posed by the current COVID-19 pandemic.[14] According to sources including a joint alert from the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the United Kingdom's National Cyber Security Centre,[15] a range and fusion of methods are being employed, such as:

- **Malware**, software intended to gain access or cause damage to a computer or network, often while the victim remains oblivious to the fact there's been a compromise;
- **Ransomware**, software designed to deny access to a computer system or data until a ransom is paid[16];
- **Man-in-the-Middle Attacks,** "cyber eavesdropping on conversations between two parties and intercept data through a compromised but trusted system;"[17]
- **Phishing,** the use of email or text messages designed to trick the victim into giving personal information that allows the criminal to steal passwords, account numbers, Social Security numbers, and access to email, bank, or other accounts;[18]

[7] CNN Business, Millions of Americans are suddenly working from home, That's a huge security risk Brian Fung, A. Marquadt, Mar 20, 2020
[8] Forbes, Data Breaches Expose 4.1 Billion Records in the First Six Months of 2019 Alone Davey Winder, Aug 20, 2019
[9] VPNOverview.com website, In the Dark
[10] Trend Micro Security Intelligence Blog, The Panamanian Shell Game: Cybercriminals With Offshore Bank Accounts? Max Goncharov, David Sancho, May 9, 2016
[11] Often with a combination of stolen, legitimate PII and fabricated documentation
[12] McKinsey, Fighting back against synthetic identity fraud Bryan Richardson, D. Waldron, Jan 2, 2019
[13] Financier Worldwide, Identifying and combatting synthetic identity fraud in financial services Apr 2020
[14] FinCEN website, The Financial Crimes Enforcement Network (FinCEN) Encourages Financial Institutions to Communicate Concerns Related to the Coronavirus Disease 2019 (COVID-19) and to Remain Alert to Related Illicit Financial Activity Mar 16, 2020
[15] DHS CISA website, Alert (AA20-099A): COVID-19 Exploited by Malicious Cyber Actors Apr 8, 2020
[16] Databreachtoday.com, 7 Ransomware Trends: Gangs Join Forces, Auction Stolen Data Mathew J. Schwartz, Jun 8, 2020
[17] Forcepoint website, What is a Man-in-the-Middle Attack?
[18] Federal Trade Commission (FTC) website, How to Recognize and Avoid Phishing Scams Updated May 2019

- **Business Email Compromise (BEC),** the use social engineering to craft email messages that appear to come from known sources making legitimate requests such as a money transfer or access to a computer network; [19] [20] and
- **Cyber-supported Fraud Schemes,** scams such as benefits fraud, charities fraud, and crowdfunding scams, which leverage email and identification (ID) issues and often typical during disasters.[21]

These cyber-related attacks on the U.S. financial system by bad actors, including nation states, state-sponsored or protected criminals, or transnational criminal organizations, are plentiful. The Federal Trade Commission (FTC) reports that from January 1, 2020, to May 21, 2020, there were 52,548 fraud complaints with a total loss amount of more than $38.6 million.[22] During this time, FinCEN has directed hundreds of COVID-19-related Bank Secrecy Act (BSA) referrals and consumer fraud alerts to law enforcement, and its Rapid Response Program, in coordination with the Department of Justice (DOJ) and the FBI, has recovered over $300 million in COVID-19-related fraud[23]. Additionally, the Securities and Exchange Commission (SEC) has suspended trading for more than 30 issuers because of accuracy and adequacy questions about COVID-19-related products and services and suspended trading for three microcap issuers due to investor-confusion concerns.[24]

Targets of Cyber-Crime Bad Actors

Cyber criminals are targeting every aspect of the financial system, including:

- **Government** – Government relief funding provided during the crisis has been one target for exploitation. Although the SBA's Paycheck Protection Program (PPP) launched on April 3, 2020, DOJ has already announced multiple PPP fraud cases. This includes two separate cases for the alleged filing of fraudulent PPP loan applications seeking more than a half-million dollars[25] and $10 million dollars[26] respectively. In both instances, defendants claimed dozens of fake employees using fraudulent or synthetic IDs at multiple shell businesses. Municipalities like Florence, Alabama, have been targets of ransomware attacks.[27] The United States Secret Service is also reviewing cases of synthetic or stolen identifications being used to defraud the Internal Revenue Service's stimulus payments program and state unemployment programs. [28]
- **Financial Institutions** – During the COVID-19 pandemic, cyberattacks to steal funds and PII against the financial sector have increased by 238 percent.[29] One important shift in such attacks is a move from 'heists' (where opportunistic criminals seek to steal data and money before exiting an environment) to 'hostage situations' (where cybercriminals aim to remain persistent on a financial institution's network for the long term).[30] Further, ransomware attacks against the financial sector have increased ninefold since the start of the crisis.[31]

---

[19] FBI website, Business Email Compromise. Accessed Jun 2020
[20] Federal Bureau of Investigation (FBI) Website, FBI Anticipates Rise in Business Email Compromise schemes related to the COVID 19 pandemic. Updated Apr 6, 2020
[21] FinCEN website, The Financial Crimes Enforcement Network (FinCEN) Encourages Financial Institutions to Communicate Concerns Related to the Coronavirus Disease 2019 (COVID-19) and to Remain Alert to Related Illicit Financial Activity Mar 16, 2020
[22] FTC website, FTC COVI-19 Complaints May 21, 2020
[23] FinCEN website, Notice Related to the Coronavirus Disease 2019 (COVID-19) pp. 4, May 18, 2020
[24] SEC website, Keynote Address: Securities Enforcement Forum West 2020 Steve Peitkin, May 12, 2020
[25] DOJ Website, Two Charged with Stimulus Fraud May 5, 2020
[26] DOJ Website, Texas Man Charged with $5 Million COVID-Relief Fraud May 19, 2020
[27] Associated Press, Alabama city to pay $300,000 ransom in computer system hack Jun 11, 2020
[28] KrebsOnSecurity.com, Riding the State Unemployment Fraud 'Wave' Brian Krebs, May 23, 2020
[29] VMware Carbon Black, Modern Bank Heists 3.0 Tom Kellermann, R. Murphy, May 2020
[30] Ibid.
[31] Ibid.

- **Third-party partners and vendors** – Bad actors are also targeting third-party partners and vendors to financial institutions. According to the May 2020 VMware Carbon Black report, "33 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." For example, ransomware attacks on FI service providers may have also been aimed at those servicers' banking-industry customers through shared points of network access.[32] [33]
- **Businesses** – Business Email Compromise (BEC), which is already the most profitable form of cybercrime,[34] has proliferated during the crisis, especially towards organizations with a role in mitigating the effects of the pandemic.[35] Further, while this method of social engineering and phishing is mostly focused on financial gain, in those schemes where a bad actor gains access to a company's network, there is also the opportunity to obtain data. The PII, especially if combined with healthcare information,[36] has a value in criminal marketplaces. Bad actors, including nation-state and state-sponsored actors, can also use these same methods to take sensitive business information and proprietary documentation (i.e., "economic espionage").[37] For example, the FBI and CISA have recently warned that the People's Republic of China has been working to infiltrate networks "to identify and illicitly obtain valuable intellectual property (IP) and public health data related to vaccines, treatments, and testing from networks and personnel affiliated with COVID-19-related research."[38]
- **Individuals** – In the wake of the COVID-19 pandemic, cybercriminals have modified traditional scams targeting individuals to emphasize COVID-19 issues and fears, to steal funds and PII or gain access to an employer's network. Often, these efforts are aimed at the most vulnerable, such as senior citizens,[39] lower-income communities,[40] and those suffering the effects of the pandemic. TransUnion research shows that "of [survey] respondents who identified themselves as being impacted due to COVID, financially laid off from work or even furloughed from work, we're seeing about 32% of those individuals also getting targeted with the COVID scams, which is more than the 22% that we're seeing with those individuals who were not financially impacted due to COVID."[41] Examples include:
    - **Imposter Scams,** which attempt solicitation of donations to steal personal information or to distribute malware by impersonating government agencies, international organizations, or healthcare organizations;
    - **Investment Scams**, which may include "pump and dump" schemes on stocks with little publicly available information or promotions that falsely claim products or services that can prevent, detect, or cure coronavirus;[42,43,44]

---

[32] KrebsOnSecurity.com, Security Breach Disrupts Fintech Firm Finastra Brian Krebs, Mar 20,2020
[33] KrebsOnSecurity.com, Ransomware Hit ATM Giant Diebold Nixdorf Brian Krebs, May 11, 2020
[34] VMware Carbon Black, Modern Bank Heists 3.0 Tom Kellermann, R. Murphy, May 2020
[35] Tech Republic, Businesses: Beware of COVID-19 email compromise scams Brandon Vigliarolo, May 7, 2020
[36] ZDnet.com, This is how hackers make money from your stolen medical data: Stolen medical information can sell for up to six times as much as PII, and there are reasons for that. Charlie Osborne, Jun 5, 2019
[37] Barron's, The Other Crisis: U.S. Companies Still Need Help Against Cyberattacks Keith B. Alexander, Jamil N. Jaffer, Mar 16, 2020
[38] FBI website, People's Republic of China (PRC) Targeting of COVID-19 Research Organizations May 13, 2020
[39] InvestmentNews.com, Scams targeting seniors are incorporating COVID-19 concerns Josh Jones, Taylor Anderson, Mar 24, 2020
[40] NPR.com, Coronavirus Payments To Poor Are Vulnerable To Fraud Tim Mak, Apr 27, 2020
[41] BankInfoSecurity.com, The State of Payments Fraud in a Pandemic Nick Holland, Jun 10, 2020
[42] SEC website, Look Out for Coronavirus-Related Investment Scams - Investor Alert Feb 4, 2020 (Updated May 21, 2020)
[43] NASAA website, The North American Securities Administrators Association (NASAA) created a COVID-19 Enforcement Task Force to review potential investment fraud from "as many as 200,000 coronavirus-related domains as of April 20, 2020. Most of these domain names appear to have been created within the past three months." NASAA Forms COVID-19 Enforcement Task Force, Apr 28, 2020
[44] USDOJ Website, Medical Technology Company President Charged in Scheme to Defraud Investors and Health Care Benefit Programs in Connection with COVID-19 Testing Jun 9, 2020

- **Product Scams,** which may come from companies selling unapproved and misbranded products making false COVID-19 health claims or those selling counterfeit or undelivered medical supplies;[45,46] and,
- **Extortion Scams,** in which a criminal demands money or information by claiming that the victim has been caught accessing embarrassing materials (e.g., adult websites) or breaking laws (e.g., immigration or copyright law).[47] [48]

Eight months ago, in October 2019, the U.S. House of Representatives passed H.R. 2513, The Corporate Transparency Act of 2019 (Maloney), with a bipartisan vote of 249-173. H.R. 2513 would close loopholes that are commonly abused by bad actors, making it harder for cyber criminals, terrorists, traffickers, corrupt officials to hide, launder, move, and use their money. This legislation also requires corporations and Limited Liability Companies (LLCs) to disclose their beneficial owners to FinCEN to end the use of anonymous shell companies for illicit activities. H.R. 2513 includes the text of H.R. 2514, The Coordinating Oversight, Upgrading and Innovating Technology, and Examiner Reform Act (COUNTER Act), a bill introduced by Mr. Cleaver (D-MO), which passed the House by voice vote. H.R. 2514 increases the number of overseas Treasury liaisons and grant money available to fight economic crimes overseas and improves public-private exchange of threat pattern and trend information to deter cyber and other types of criminals that operate around the globe.

Legislative Proposals

- **H.R. ____, Internet Fraud Prevention Act** (Sherman). This bill would: require the Federal Reserve, Federal Trade Commission, and FBI to study and report on BEC scams and provide potential solutions; direct the Federal Financial Institutions Examination Council to include BEC in its BSA/AML Examination Procedures; and create a Real Estate Fraud Advisory Group to develop model BEC educational materials for use by industry participants.
- **H.R. ____, COVID-19 Restitution Assistance Fund for Victims of Securities Violations Act** (Wexton). This legislation would create a fund at the Securities and Exchange Commission to provide restitution payments for individuals in connection with securities fraud related to coronavirus if they do not otherwise receive full payment of restitution.
- **H.R. ____, Senior Investor Pandemic and Fraud Protection Act** (Gottheimer). This legislation would amend the Consumer Financial Protection Act of 2010 to authorize grants to States to protect seniors and vulnerable adults from misleading and fraudulent marketing or sales practices related to the COVID–19 pandemic and other unlawful scams.
- **H.R. ____, To require the Federal financial regulators to issue guidance to encourage depository institutions to establish programs to educate customers at risk of unwittingly becoming money mules** (Gabbard). This bill aims to raise awareness among vulnerable communities which are targeted to be "money mules" to transfer illegally acquired funds on behalf of or at the direction of a bad actor.

[45] FTC website, FTC & FDA: Warnings sent to sellers of scam Coronavirus treatments Mar 9, 2020
[46] KrebsOnSecurity.com, Unproven Coronavirus Therapy Proves Cash Cow for Shadow Pharmacies Brian Krebs, Apr 24, 2020
[47] FBI IC3 website, Online Extortion Scams Increasing During The Covid-19 Crisis Apr 20, 2020
[48] KrebsOnSecurity.com, Tech Support Scam Uses Child Porn Warning Brian Krebs, May 7, 2020