Michael D'Ambrosio

Assistant Director
Office of Investigations
United States Secret Service

Prepared Testimony on
"COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic"

Before the
United States Senate
Committee on the Judiciary
June 9, 2020

Intro

Thank you Chairman Graham, Ranking Member Feinstein, and the Members of this distinguished Committee for holding this important hearing, and for inviting me to speak about the work of the U.S. Secret Service to counter cyber and financial crimes exploiting the coronavirus pandemic.

As early as February of this year, the U.S. Secret Service identified individuals and groups seeking to exploit the pandemic to further fraudulent schemes for their illicit profit. We published our first alert on this subject, on March 4, 2020, which focused on phishing schemes. As the pandemic continued and intensified, we have observed a proliferation and diversification of criminal schemes, particularly an increase in targeting various economic relief programs, such as those provided by the CARES Act. Countering this fraud has become a core focus of our investigative work, and I expect our investigative efforts to recover stolen assets and hold criminals accountable will continue for years.

The Secret Service, in addition to our protective mission, is responsible for the investigation of criminal violations of U.S. law pertaining to the U.S. financial system, including traditional financial crimes (such as wire fraud and money laundering), modern computer crimes (such as crimes associated with digital currencies), as well as counterfeiting of currency and other financial instruments.

As the Assistant Director of the Office of Investigations, I lead the over 160 field offices of the Secret Service, which include our network of electronic and financial crimes task forces, which conduct specialized investigations of computer and financial crimes. As a result of the pandemic, the risks to our financial system have evolved and multiplied, and we have taken swift action to adapt our work to continue safeguarding the integrity of financial systems from threats to our national and economic security.

In my testimony today, I'd like to the take the opportunity to describe how these risks have evolved, what the Secret Service is doing to combat them, and how we are working with partners across the Nation, and around the globe, to safeguard the integrity of financial systems, and, ultimately, to hold criminals accountable.

The Risk of Cyber-Enabled Fraud

Major disasters have long invited fraud. From the terrorist attacks on 9/11 to Hurricanes Katrina and Maria – and indeed well before – criminals throughout history have exploited emergencies for illicit gain. The more catastrophic the event, the more active the fraudsters.

However, the fraud associated with the current COVID-19 pandemic presents a scale and scope of risks we have not seen before. While a hurricane may impact multiple states and thousands of people, this global pandemic impacts everyone. Enabled by the Internet, criminals all over the world are exploiting the fear and uncertainty of the moment for their own illicit gain. They are defrauding anxious citizens, distressed businesses, and government stimulus programs alike. And they will continue to do so throughout the course of this pandemic and the following recovery.

Over the course of the past few months, the Secret Service has observed a clear evolution of the types of frauds being perpetrated. Our first alert, on March 4, 2020, warned of increasing use of COVID-19 themes in "phishing" campaigns. Phishing is the practice of sending emails, purporting to be from reputable companies or organizations, in order to entice individuals to reveal personal information, such as passwords and credit card numbers, or to unknowingly download malicious software. Phishing is a longstanding criminal tactic online. However, as people and organizations have adapted to teleworking, people have become increasingly susceptible to fraudulent emails exploiting their concerns about this pandemic.

But phishing was just the beginning. Over the subsequent weeks, the crimes exploiting the pandemic began to diversify and substantially increase.

As communities sought out legitimate medical equipment to treat and prevent the spread of COVID-19, criminals began to peddle fraudulent medical equipment. Fraudsters engaged in "non-delivery" scams, in which payment is sent for goods and/or services, but no goods or services are ever delivered.

As anxious citizens sought out COVID-19 testing, criminals stood up sham testing sites, both to collect "fees" for fraudulent testing and to collect personal information that could later be used in identity theft and other frauds. They began peddling fake cures, substandard masks, and fraudulent tests.

As workers across the country increasingly turned to telework to increase social distancing, criminals began deploying ransomware, software designed to extort money by locking a computer system until a ransom is paid.

And they engaged in business email compromise (BEC) scams, sophisticated frauds designed to deceive businesses into sending large sums of money into the bank accounts of criminals. With workers out of the office, many of the normal oversight mechanisms that have might otherwise have prevented an organization from becoming a victim, such as in-person approval for wire transfers, made organizations especially susceptible to BECs.

Finally, as the Federal Government began to dispense stimulus funds, primarily through CARES Act programs, criminals launched a new wave of schemes aimed at defrauding U.S. and state government agencies, financial institutions, businesses, and even individuals, out of taxpayer dollars intended to support our fellow citizens, businesses, and communities in need.

The fraud related to the CARES Act is perhaps the most troubling development thus far. Congress has appropriated nearly $3 trillion to support the American economy, the largest-ever economic stimulus package in U.S. history. Even if we assume a very low rate of fraud, of just 1%, we should still expect more than $30 billion will end up in the hands of criminals. And that is likely an underestimation of the risk, and just one portion of the full range of risks at play. This is why countering criminal schemes seeking to exploit the COVID-19 pandemic has become a primary investigative focus for the U.S. Secret Service, and will remain so over the coming years.

Strategy

The Office of Investigations is currently focusing on four broad categories of COVID-19-related crime, and has numerous ongoing investigations related to each of these categories. These four categories are:

1. COVID-19-related scams, including the sale of fraudulent medical equipment and non-delivery scams;
2. Risks of cyber crime resulting from increased telework nationally, such as BECs;
3. Ransomware and other cyber-criminal activity that could disrupt the pandemic response; and,
4. Defrauding of government and financial institutions associated with response and recovery efforts.

It is this fourth category that I think is of particular interest to this Committee. It is an area the Secret Service is devoting extraordinary investigative effort to addressing. It is despicable that some seek to engage in fraud against U.S. government programs that aim to brunt COVID-19-induced economic harms. This includes fraud against unemployment benefits, Economic Impact Payments (EIPs), Paycheck Protection Program (PPP) funds, and other CARES Act initiatives. These criminals aren't just defrauding these programs directly, but also impeding the execution of these programs, thus denying essential aid to intended recipients in dire need of assistance.

I am pleased to report that Secret Service has already seen tremendous success emerge from our investigative efforts to date. We have initiated over one hundred criminal investigations and prevented approximately $1 billion in fraud losses.

Among other law enforcement actions, the Secret Service has successfully disrupted hundreds of online COVID-19-related scams,[1] halted the alleged illicit sale of stolen COVID-19 test kits online,[2] and is participating in a nation-wide effort to counter a vast international scheme[3] to defraud U.S. state unemployment systems. We have also released regular threat intelligence and alerts[4] to provide industry, consumers and our law enforcement partners with best practices[5] to defend themselves from the latest criminal threats.

The immediate investigative focus of the Secret Service is to disrupt and deter criminal activity that could hinder an effective response to the pandemic, to assist organizations at risk of crime, and to recover any funds stolen from Americans. Longer term, we will work to ensure that those who have criminally exploited this crisis are arrested and successfully prosecuted.

[1] https://www.justice.gov/opa/pr/department-justice-announces-disruption-hundreds-online-covid-19-related-scams
[2] https://www.justice.gov/usao-wdpa/pr/new-york-city-man-arrested-fraud-charges-selling-stolen-covid-19-testing-services
[3] https://www.nytimes.com/2020/05/16/us/coronavirus-unemployment-fraud-secret-service-washington.html
[4] https://www.secretservice.gov/data/press/releases/2020/20-APR/Check-Security-Features-for-Economic-Impact-Payments.pdf
[5] https://www.secretservice.gov/data/press/releases/2020/20-MAR/Secret_Service_Coronavirus_Phishing_Alert.pdf

Partnerships

Yet the Secret Service never operates alone. We work with a range of government and industry partners in executing our mission. In particular, the various agencies of the Department of the Treasury, including the Financial Crimes Enforcement Network (FinCEN), the Internal Revenue Service (IRS), the Treasury Inspector General for Tax Administration (TIGTA), and the various Offices of Inspectors General, including from the Department of Labor, are all critical partners in safeguarding the integrity of U.S. financial systems.

In addition, given the importance of the PPP, we are partnering with the Office of the Inspector General (OIG) of the Small Business Administration (SBA) to combat fraud against business loans. The Secret Service and SBA OIG have brought together the combined authorities, capabilities, tools, and human resources of our respective agencies in order to combat PPP-related fraud at both the national and local levels.

And, of course, to effectively coordinate across the whole of the U.S. government, we are actively engaging with the Department of Justice's COVID-19 task forces, the Federal Bureau of Investigation, Homeland Security Investigations, the Cybersecurity and Infrastructure Security Agency (CISA), and other law enforcement agencies at the state, local, and federal levels, both in the United States and abroad.

Lastly, we have dramatically expanded our outreach to industry, particularly America's financial institutions, which are responsible for distributing much of the CARES Act funds to the public. With the financial institutions, we have expanded our information sharing and other cooperation to rapidly detect fraud, freeze assets, and return money to government agencies and others who have been defrauded. This cooperation is absolutely essential, given the ability of the financial institutions to intercede quickly in the event of fraud.

Conclusion

The ongoing spate of COVID-19-related crime is in many ways a culmination of years of mounting risk within the financial sector, driven in large part by the growth of transnational cyber-crime. COVID-19-related frauds are made possible by the persistent effort by cyber-criminals to breach computer systems to steal personal information, which can subsequently be used to fraudulently apply for loans and benefits payments. Recent data breaches have allowed criminals to buy and sell this information, such as social security numbers and account passwords, which can later be used in an extensive range of frauds.

But the insecurity of the digital realm is not solely a matter of economics. These same criminals are also assisting nation-states in activities that present a very real threat to America's national security. Over the past twenty years, there has been a steady growth in transnational cyber-crime, and cooperation between these transnational criminal organizations and some foreign states. What we are seeing now with this pandemic is an acceleration of this trend, which is coinciding with a vulnerable moment for our nation and our economy. I am committed to countering this sort of criminal activity and look forward to answering your questions on how we can work together to address this threat.