WRITTEN TESTIMONY

OF

David Smith
Assistant Director, Office of Investigations
United States Secret Service

BEFORE

Committee on Oversight and Accountability
United State House of Representatives

ON

"Federal Pandemic Spending: A Prescription for Waste Fraud and Abuse"

February 1, 2023
Washington, DC

Introduction
Good morning, Chairman Comer, Ranking Member Raskin, and distinguished Members of the Committee. Thank you for the opportunity to appear before you today and discuss the ongoing efforts of the U.S. Secret Service (Secret Service) to protect the nation's financial infrastructure.

I serve as the Assistant Director for the U.S. Secret Service, Office of Investigations. In this role, I oversee our 161 field-based offices and several headquarters divisions that execute all aspects of our integrated mission, including our criminal investigations. I also direct our 42 Cyber Fraud Task Forces, located in our largest offices, and our National Computer Forensics Institute in Hoover, Alabama, which trains local law enforcement, prosecutors, and judges.

For more than 150 years, the Secret Service has conducted criminal investigations to protect the American public, financial institutions, private companies, and critical infrastructure from exploitation. We've done so while also fulfilling our diverse protective requirements around the world. Financial crimes are increasingly transnational in nature and cyber-enabled. We work persistently to maximize our effectiveness at safeguarding financial institutions and payment systems from criminal exploitation.

Combating Pandemic Fraud
In recent years, countering COVID-19 pandemic-related fraud has absorbed a substantial portion of our investigative attention and resources. It is our duty to detect and arrest criminals, seize their illicitly gained assets, and dismantle the infrastructure they rely upon to enrich themselves. We have been working to hold criminals accountable for pandemic-related fraud since the spring of 2020.[1] No different than other current and emerging cyber-enabled financial crimes, these criminals have leveraged technology in several ways to effect pandemic-related fraud schemes. The pandemic reaffirmed the need to continue evolving in our application of technology, training, and analytical tools to combat contemporary criminal activities and trends.

During the early stages of the pandemic, I served as the Special Agent in Charge of our Criminal Investigative Division, the hub for all major investigative efforts. At the inception of the pandemic, I was at the center of our agency's national and global coordination efforts with law enforcement and industry partners. Prior to the enactment of the CARES Act (P.L. 116-136) in March 2020, we reached out to other government entities, such as the U.S. Small Business Administration's (SBA) Office of the Inspector General (OIG), the Department of Labor OIG, the Department of Health and Human Services' OIG, the Council of the Inspector Generals on Integrity and Efficiency, the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN), and many others. We understood that many key partners in this effort had limited resources, and the best way to address the looming wave of potentially fraudulent activity was to do so collectively, and to dedicate a wide range of resources. We also worked with several longstanding partners in fighting financial crimes within the Department of Justice (DOJ) and coordinated with U.S. Attorney's Offices around the country to ensure consequences for criminals.

[1] D'Ambrosio, Michael and Wade, Terry, "There's another coronavirus crisis brewing: Fraud." (Washington Post, 14 April 2020). Accessed 18 January 2023 at: https://www.washingtonpost.com/opinions/2020/04/14/theres-another-coronavirus-crisis-brewing-fraud/

Our well-established and trusted relationships with financial institutions stemming from our origins in combating the spread of counterfeit U.S. currency afforded us the agility to seize the reigns on countering pandemic-related fraud. We are a relatively small agency with a critical national security role and focused jurisdictional responsibilities. While we are proud and confident, we recognize that our mission has required our partners to be fully engaged with us.

As a 20-plus year law enforcement professional, the exploitation of well-intentioned programs, resources, and tools for personal gain is not new to me. My colleagues and I have seen and countered the full spectrum of pandemic-related fraud to date. From N-95 mask non-delivery schemes to synthetic accounts used in identity theft scams to apply for millions of dollars in loans. From medical facilities targeted with ransomware attacks at the height of the pandemic to prison inmates applying for unemployment benefits. Moreover, numerous cases have involved insiders or others holding trusted positions within their organizations with access to victims' personal data abusing that authority and access.

The volume of fraudulent activity related to CARES Act funding was and is substantial, yet a similar dynamic has been seen before with other major relief efforts or natural disasters. The COVID-19 public health crisis presented an opportunity for both organized criminal groups and individuals intent on taking advantage of these important resources. As Congress enacted legislation to provide relief and stability to the American public and the economy, the Secret Service began its outreach to mitigate the potential misuse of pandemic relief funds.

Our Cyber Fraud Task Forces connected with U.S. Attorney's Offices and other federal counterparts in every jurisdiction to ensure that all parties had the most relevant information on criminal trends and tactics targeting pandemic relief funds. We worked with partners in the financial sector, such as FinCEN and the National Cyber-Forensics Training Alliance, to identify indicators of compromise. We issued numerous advisories to financial institutions as new information developed, to include ways to prevent and mitigate pandemic-related fraud. Our joint advisories reached nearly 30,000 financial institutions. Through these advisories and our field work, we assisted in returning approximately $3 billion to unemployment insurance benefits.

While the Secret Service had a major hand in whole-of-government coordination, we also pivoted internally to address the looming surge of potential pandemic-related fraud. We mobilized our field offices and Cyber Fraud Task Forces, with support and coordination provided by our Global Investigative Operations Center and our Asset Forfeiture team. Thanks to our dedicated special agents, analysts, and support staff, we were able to launch quick and efficient investigations. Our success was also made possible by the critical partnerships maintained nationwide with federal, state, local, tribal, and territorial (SLTT) government organizations and law enforcement agencies, as well as private sector partners. For example, federal agencies have and continue to provide crucial support in identifying fraudulent cases by facilitating the sharing of data and referral of suspect cases to OIGs for further investigation.

Since 2020, the Secret Service has seized for forfeiture over $1.43 billion in fraudulently obtained funds pursuant to 18 U.S.C § 981 and 982.

The Secret Service has initiated more than 2300 unemployment insurance fraud investigations and investigative inquiries, as well as 2900 SBA program fraud investigations and investigative inquiries.

Investigative Efforts

One of our earliest efforts, still ongoing, was an investigation by our Denver Field Office Cyber Fraud Task Force into crimes targeting SBA Economic Injury Disaster Loan (EIDL) funds. We initiated this investigation in October 2020, in consultation with DOJ. We formed a task force with the U.S. Attorney's Office for the District of Colorado, with a focus on identifying and prosecuting large-scale criminal organizations and seizing illicitly gained EIDL funds. Our investigation revealed that the funds were being fraudulently obtained by using fabricated or stolen employment and personal information to receive loans. The investigation also revealed that these criminals exploited multiple pandemic relief programs. This effort would not have been possible without the support of SBA OIG and the Pandemic Response Accountability Committee (PRAC). To date, the Secret Service has returned approximately $286 million in fraudulently obtained EIDL funds recovered from over 15,000 fraudulent accounts to the SBA and seized over $1 billion in EIDL funding.

Another example is a case from June of 2020, where a criminal ring based in South Florida applied for and received $24 million in pandemic relief funds by using synthetic identities and shell companies. The synthetic identities were manufactured years earlier to commit other bank and credit card fraud. The criminals used personal and financial information of real people, such as stolen Social Security numbers, with false names and other identifiers. This investigation demonstrates the significance of our Cyber Fraud Task Forces, which partner with other law enforcement agencies and financial institutions to identify and counter financial crimes. Together, we were able to identify numerous businesses, bank accounts, and illicit funds connected to this group, and bring consequences to the co-conspirators. To date, approximately $11 million has been seized for forfeiture, with additional seizures anticipated.

Several state unemployment benefit agencies were targeted in the early months of the pandemic. For example, in May of 2022, our Atlanta Field Office Cyber Fraud Task Force identified thousands of such fraudulent claims, totaling more than $30 million, using stolen identities and Social Security numbers from Americans in the agricultural, education, and medical fields. We believe that a criminal group stole these identities from a variety of sources, with at least 1,600 coming from an insider with access to hospital databases. Total losses in this case now stand at over $80 million. Eight defendants have been indicted to date for their roles in the scheme, and the investigation continues.

The final case I would like to highlight is from July of 2020 where a group of individuals, to include inmates at state and county penal institutions in Pennsylvania, illegally obtained unemployment benefits. The inmates worked with co-conspirators to claim unemployment benefits by using their real identities and making false statements. This investigation resulted in the arrest of 10 co-conspirators, and over $136,000 paid in restitution.

Lessons for the Future

Our work combating pandemic fraud has underscored some important reminders:

1) Cybercrime is financial crime: To safeguard Americans from online crimes, we have to look at a wide range of options to improve law enforcement's ability to detect illicit activity online and deny criminals the proceeds of their illicit activity. The Attorney General made important recommendations in his report pursuant to Executive Order 14067, Ensuring Responsible Development of Digital Assets.[2]
2) Fraudsters will exploit disasters: While the particular fraud schemes will vary, the Secret Service and its law enforcement partners will need to maintain a robust ability to deter, detect, and disrupt fraud schemes. This capacity can't be built reactively in response to a particular disaster; it must be standing and continually engaged to disrupt and deter those that engage in fraud. Unfortunately, reports show a continued decline in federal white-collar crime prosecutions.[3]
3) Collaboration is paramount: The small team at a particular OIG office or an auditor at a financial institution should not be expected to detect and combat sophisticated fraud schemes alone. Collaboration between law enforcement agencies, both domestic and international, and with the private sector, is essential for combating modern crimes. The work of our Cyber Fraud Task Forces and our National Computer Forensics Institute are critical parts of fostering such collaboration.

Conclusion

In conclusion, I am honored to represent the dedicated professionals of the Secret Service. They work tirelessly on behalf of the American people and continue to maintain our standing as one of the world's preeminent law enforcement organizations.

As with other relief fund frauds, I expect that our investigative efforts to recover stolen assets and hold criminals accountable for pandemic fraud will continue for years to come. At the same time, the Secret Service will continue to confront evolving threats targeting our financial critical infrastructure. With the continued support of Congress and the Department of Homeland Security, I am confident the men and women of the Secret Service will remain prepared to address the substantial demands of our integrated mission.

Thank you again for the opportunity to appear before you to discuss the Secret Service's ongoing efforts to counter COVID-19 related fraud and other cyber-enabled financial crimes. We welcome your partnership and counsel, and now I look forward to taking your questions.

[2] U.S. Department of Justice, "The Report of the Attorney General Pursuant to Section 5(b)(iii) of Executive Order 14067: The Role Of Law Enforcement In Detecting, Investigating, And Prosecuting Criminal Activity Related To Digital Assets" (Washington, DC, 6 September 2022). Accessed 18 January 2023 at: https://www.justice.gov/media/1245466/dl

[3] TRAC Reports, "White-Collar Crime Prosecutions for 2021 Continue Long Term Decline" (9 August 2021). Accessed 18 January 2023 at: https://trac.syr.edu/tracreports/crim/655/