Jason D. Kane

Special Agent in Charge
United States Secret Service

Prepared Testimony

Before the
United States House of Representatives

Homeland Security Committee
Subcommittee on Counterterrorism, Law Enforcement, and Intelligence

Regarding a Hearing on

Organized Retail Crime

December 12, 2023

Introduction

Chairman Pfluger, Ranking Member Magaziner, and distinguished members of this Subcommittee: Thank you for inviting me to testify before you on the current investigative capabilities of the U.S. Secret Service (Secret Service) and how they may be of help addressing the rising trend of organized retail crime (ORC).[1]

As one of the nation's original investigative agencies, charged with safeguarding the nation's financial and payment systems, the Secret Service has, since 1865, conducted criminal investigations to protect the American public, financial institutions, and critical infrastructure from criminal exploitation. As early as 1982, the Secretary of the Treasury directed the Secret Service to investigate crimes related to electronic funds transfers to keep pace with the growing role of computers in the U.S. financial system. Today, we have extensive authorities to safeguard financial payment systems from criminal exploitation, even as those illicit activities are increasingly transnational in nature and enabled by cyberspace and digital currencies.

I currently serve as the Special Agent in Charge of the Nashville Field Office with oversight of middle and eastern Tennessee. In my former role as a Deputy Assistant Director, I helped drive our investigative focus and priorities supporting our 161 field offices. I drafted polices for our offices to deploy, but now I implement those polices to deter, disrupt, and ultimately prosecute actors involved in transnational criminal organizations (TCOs).

In executing our law enforcement mission, the Secret Service closely partners with Federal, state, local, tribal, territorial, and international law enforcement agencies. We do this in part through our network of Cyber Fraud Task Forces (CFTFs)[2] which are strategically placed in major cities across the United States. In criminal investigations involving digital currency, we partner particularly closely with Homeland Security Investigations (HSI), the Financial Crimes Enforcement Network (FinCEN), the Federal Bureau of Investigations (FBI), the Department of Justice, and other Federal agencies with related responsibilities as well as state and local law enforcement partners.

The Secret Service's primary areas of focus with respect to combating organized retail crime are in training our state and local partners, providing shared resources in the form of technical tools, and utilizing our specialized abilities to track and seize illicit funds, often in the form of

[1] ORC is the large-scale theft of retail merchandise with the intent to resell the items for financial gain. National Retail Federation, https://nrf.com/advocacy/policy-issues/organized-retail-crime.

[2] Section 105 of the USA PATRIOT Act of 2001 directed the Secret Service to establish a "a national network of electronic crimes task forces, … for the purpose of preventing, detecting, and investigating various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems." The first Secret Service Electronic Crimes Task Force (ECTF) was established in New York in 1995; today the Secret Service operates 42 domestic CFTFs, as part of an expanding international network that partners Federal, state, and local law enforcement with the private sector and academia to effectively investigate cybercrimes.

cryptocurrencies, which are used by TCOs to conceal and transfer their ill-gotten gains. The Secret Service has an exceptional record of success in disrupting TCOs, and we remain committed to keeping pace with both technology innovation and the evolving strategies and tactics of cyber criminals. My testimony today will explain our efforts, and the challenges we face, in addressing organized retail crime and related criminal activity.

Impact of National Computer Forensics Institute (NCFI)

The Secret Service identified the availability of cyber-related training and equipment at the state, local, and tribal levels as an issue in the early 2000s. Established in 2008, through a partnership initiative between the Department of Homeland Security (DHS), the Secret Service, and the Alabama District Attorneys Association, the NCFI has trained more than 24,000 state, local, tribal, and territorial (SLTT) law enforcement, prosecutors, and judicial officials. Trainees hail from more than 4,700 agencies throughout all 50 states and five U.S. territories. Since 2017, the NCFI has issued more than $122 million in computer equipment to SLTT digital forensics examiners. This equipment is sent back to SLTT departments and used to investigate a wide spectrum of crime, to include retail crime.

The impact of the NCFI's training mission on SLTT law enforcement partners is evident firsthand through the Forensic Partner Reporting program. Graduates of NCFI's forensic examiner courses utilize Secret Service-issued equipment to conduct examinations in a wide range of criminal investigations across the nation, and report back on their work. Reporting for Fiscal Year (FY) 2023 is at an all-time high, reflecting that SLTT partners conducted over 200,000 exams and analyzed more than 35 petabytes of data, which is the equivalent of 700 million four-drawer file cabinets full of data. More than half of all exams reported involved violent crime investigations, to include homicide, robbery, rape, and child exploitation.

Cases today revolve around the ability to prove guilt in a cyber environment. I would submit to you that 25 years ago cases regularly hinged on biological DNA evidence as the pillar of a prosecution. Today, cases also regularly rely on "computer DNA" or "digital dust" from computer forensics to show the pattern and intent of criminal actors and their networks. Without this type of evidence, many criminal actors may go free or receive limited sentences as the full degree of their culpability is not discovered. Last year, Congress renewed its commitment to the NCFI program by passing legislation that expanded this program and allowed for its continued operation through the end of FY 2028. This legislation has strengthened the capabilities of the Secret Service and our law enforcement partners to combat modern criminal activity, including organized retail crime.

Cyber Fraud Task Forces & Partnerships

Our Cyber Fraud Task Forces are connected with U.S. Attorneys' Offices and other federal SLTT counterparts in every jurisdiction to ensure that our partners have the most relevant information on criminal trends and tactics used by organized criminal groups. Our well-established and trusted relationships with financial institutions, stemming from our origins in combatting the spread of counterfeit currency, affords us the agility to aid with cases involving organized retail crime. We are fully engaged with our partners, as partnership is essential to accomplishing our mission.

We work daily with partners in the financial sector, such as FinCEN and the National Cyber-Forensics Training Alliance (NCFTA), to identify trends throughout the country. We issue advisories to financial institutions as new information is developed, to include ways to prevent and mitigate fraudulent schemes. While the fight remains, a tangible example of our CFTF capabilities were shown during the COVID-19 pandemic, where we seized and returned over $1.65 billion in fraudulently obtained Small Business Administration loans and unemployment insurance benefits and arrested more than 670 individuals.

Lastly, to ensure we are an effective partner to the private sector, we have placed renewed emphasis on public outreach. One item I have personally learned in my tenure with this agency is that our private sector partners are in this fight with us. We have increased our outreach initiatives in the form of podcasts, in-person briefings, and our first-ever citizens academy, which was hosted by our Dallas Field Office just a few months ago.[3] Addressing cyber enabled crime is a team sport, and we rely heavily on close collaboration with stakeholders, just as we do when we complete our protective mission.

Strategy

The Office of Investigations Strategy, FY 2021-2027, identifies the following three objectives to safeguard U.S. financial systems:

1. Detect, investigate, and arrest those committing financial crimes.

2. Identify and seize assets to prevent illicit profit and recover victim financial losses.

3. Strengthen the ability of stakeholders to prevent financial crimes.

It is in the second category that I believe may be of particular interest to this committee. It is an area the Secret Service has and continues to devote extraordinary effort to staff, resource, and train our personnel to address. I am pleased to report this fight is one the Secret Service takes on daily, and we have numerous examples of how our strategies are working. Based on our efforts,

[3] https://www.secretservice.gov/newsroom/behind-the-shades/2023/08/secret-service-pilots-citizens-academy-dallas.

we prevented over $2.6 billion in fraud in FY 2022.[4] These losses are victim based and attributable to crimes such a Business Email Compromises (BECs), romance scams, and stolen personal information via Dark Web marketplaces.

Without effective law enforcement intervention, consumers will bear the brunt of higher cost for items based on the acts of criminal groups. These criminals are not only defrauding retailers but also impeding the availability of commerce as retailers are unable to fight the problem alone.

Investigative Efforts

The immediate investigative focus of the Secret Service is to disrupt and deter criminal activity and to recover any funds stolen from Americans. Longer term, we work to ensure that those who have criminally exploited our businesses are arrested and successfully prosecuted. Cyber-enabled crimes are often transnational and multi-jurisdictional in nature, which is why Federal assistance is many times not only warranted, but it is essential.

While much of our casework does not directly involve retail theft, we support efforts to counter ORC through our investigations involving the illegal movement of money. Today, much of that money laundering is facilitated through digital assets. I think back to a case involving Liberty Reserve, which was designed to facilitate illegal transactions and launder the proceeds of various crimes.[5]

While we shut down Liberty Reserve in 2013, just last month, the Secret Service worked with a cryptocurrency company to freeze $225 million worth of assets related to a transnational criminal scheme.[6] It is the intention of the Secret Service to seize the funds associated with illegal activity in this case and return as much as possible to victims. In FY 2022 and 2023, we returned over $570 million to victims of crime. Our actions to address illicit financial activity will undoubtably deal a financial blow to those engaged in ORC by limiting their ability to use the proceeds from selling stolen items.

Operation Urban Justice

In late 2022, the Secret Service entered a prolific investigation involving the State of California and the theft of Electronic Benefit Transfer (EBT) benefits. The EBT program was being exploited by organized crime groups and the direct losses at the time of case inception was approximately $90 million. This coordinated effort sought to target transnational organized

[4] USSS Annual Report, FY22.
[5] Office of Public Affairs, "Liberty Reserve Founder Sentenced to 20 Years for Laundering Hundreds of Millions of Dollars" (U.S. Department of Justice 6 May 2026). Accessed 30 November 2023 at: https://www.justice.gov/opa/pr/liberty-reserve-founder-sentenced-20-years-laundering-hundreds-millions-dollars.

criminals who were skimming EBT cards from local retailers and using the stolen numbers to steal funds from the intended beneficiaries who rely upon these subsistence benefits. The operation itself combined the efforts of over 400 law enforcement personnel from USSS, HSI, DOJ, and our California State and local partners. The State was also losing around $9 million a month as the criminal groups were exploiting the monthly benefits as they were loaded onto the true recipient's accounts.

Operation Urban Justice was conducted on March 1, 2023, and yielded 15 Federal arrests, over $100K in cash seized, 40 encoded cards, and numerous cell phones used for the operation which we have now used to identify additional elements of the TCO. This effort required the use of artificial intelligence-based technologies and data analytics to wade through reems of financial and video data from months of exploitation by these TCOs. The Secret Service will continue to go after those who will use the Governmental programs designed for the intended beneficiaries who rely upon these subsistence benefits and hold them accountable. This is a tailored example of how we address TCOs daily.

Challenges

While the Secret Service does not have a lead role in the effort to fight organized retail crime, this crime does have commonality with other contemporary crimes in the use of computers, transnational co-conspirators, and the illicit financial activity. These groups are commonly technically savvy and know how to move their funds outside of the purview of traditional money laundering pathways. This is no longer the days of Sammy "The Bull" Gravano laundering quarters through laundromats; this is moving millions of dollars' worth of assets transnationally and electronically within seconds.

One area where Congress could help is by amending 18 U.S.C. § 3056 to authorize the Secret Service to investigate those involved in criminal violations of 18 U.S.C. § 1960, and related illicit financial activity occurring in financial institutions which are regulated under the Bank Secrecy Act, but do not meet the definition of "federally insured financial institution" under Title 18 of the U.S. Code.[7] In May 2023, DHS sent the proposed amendment to 18 U.S.C. § 1960 to Congress for consideration. The Secret Service continues to engage members of both the House and Senate, to explain the purpose and nature of this legislation. In short, our financial systems, and our mission, has evolved since 1865, and our authorities must keep pace so we can effectively address new forms of illicit activity.

Conclusion

[7] Reference the definition of "financial institution" in 31 U.S.C. § 5312, compared to the definition in 18 U.S.C. § 20, and the phrase "federally insured financial institution" used in 18 U.S.C. § 3056(b)(3).

In conclusion, I am honored to represent the dedicated men and women of the Secret Service here today. 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.

The Secret Service will continue to partner with HSI to hold criminals accountable and seize illicit gains to deter further criminal activities and compensate victims. At the same time, the Secret Service will continue to be on the leading edge of evolving threats targeting the financial infrastructure, a post we have held since 1865.

I truly appreciate the chance to represent the Secret Service and discuss some of the ways we can aid in the pursuit of cyber- enabled crime, including organized retail crime. The Secret Service appreciates your partnership and guidance, and I welcome any questions the committee may have.