Statement by
The Honorable John Walk
USDA Inspector General
Submitted to the Delivering on Government Efficiency Subcommittee
Oversight and Government Reform Committee
U.S. House of Representatives

Chairman Burchett, Ranking Member Stansbury, and Members of the House Oversight and Government Reform Committee, Subcommittee on Delivering Government Efficiency, thank you for inviting me to testify on Supplemental Nutrition Assistance Program (SNAP) fraud. I am pleased to offer my perspective on this important issue as the Inspector General of the U.S. Department of Agriculture (USDA). SNAP fraud is a reprehensible crime that squanders the compassion of American taxpayers who fund the program and robs from those low-income Americans who qualify for SNAP benefits to feed themselves and their families. My testimony today will provide an overview of SNAP, examine different kinds of SNAP fraud, and discuss ways in which SNAP fraud can be deterred on the State and Federal level.

SNAP fraud has evolved. It is not confined to a single individual who engages in deceptive practices to apply for SNAP benefits for which they are not eligible. Perpetrators of SNAP Fraud include highly organized, tech-savvy, sophisticated criminals that steal enormous sums of money. Proceeds of SNAP fraud have gone to individuals linked to terrorist groups, foreign adversary nations, and transnational criminal organizations.

SNAP Overview

SNAP is the nation's largest domestic food assistance program. In fiscal year (FY) 2024, the program served 41.7 million individuals in an average month at an annual Federal cost of over $100 billion. SNAP benefits may be used to buy eligible food at more than 250,000 USDA authorized retailers nationwide. With Federal regulatory oversight, administration of SNAP at the local level is managed by State agencies that review applications and determine if households qualify for assistance. Benefit amounts are based on household size and financial circumstances. SNAP benefits are issued to recipients on electronic benefits transfer (EBT) cards monthly. Program participants may purchase food in exchange for SNAP benefits at retail locations.

SNAP fraud is not a victimless crime, although its victims are often forgotten. Not long after becoming Inspector General, one of my Special Agents shared with me the story of a SNAP recipient, a mother of four, who discovered that her SNAP benefits were stolen from her EBT card while attempting to pay for food at the grocery store. In tears, she reported the crime and asked how she would feed her family for the month until benefits would next be paid out. In another instance, a victim said her three children had to consume food that was obtained from food banks for an entire month while she and her husband consumed minimal food after her SNAP benefits were stolen. One complaint from our hotline alleged that someone in New Jersey had hacked her electronic transfer benefits. The victim did not know anyone in New Jersey, nor did she authorize the $318 in transactions made, which left the victim with nothing on her EBT card. The victim continued, "This is unfair to my 8-year-old child and I, now leaving us desperately hungry for 30 days until reimbursement." The effects of SNAP fraud are far-reaching and can have devastating impacts. OIG is committed to finding the bad actors that steal innocent victims' benefits and working with prosecutors to bring them to justice, thereby restoring integrity to SNAP so that families who appropriately rely on SNAP benefits do not have to go hungry.

SNAP Fraud

In providing SNAP oversight, OIG uses a multi-pronged approach that involves our Office of Investigations, Office of Audit, and Office of Analytics and Innovation. Our Office of Investigations employs specific law enforcement authorities, tools, and techniques to conduct SNAP fraud investigations, and this work is intended to result in appropriate actions to resolve allegations and to prevent and deter instances of illegal or fraudulent acts or misconduct. Our Office of Audit conducts reviews of SNAP intended to improve USDA's administration of the program. Our Office of Analytics and Innovation uses data analytics and tools to identify patterns of fraud and support the work of investigators and auditors.

Due to limited time, I will highlight some of the prevalent forms of SNAP fraud, though we constantly monitor efforts to create or exploit vulnerabilities in SNAP administration that can emerge at any time.

With the rise in the use of electronic benefits information technology, fraud schemes are becoming more advanced, exploiting modern financial payment systems. Many news outlets

have reported on the widespread scheme known as EBT card skimming. Card skimming occurs when criminals install illegal skimming devices on, for example, ATMs, gas pumps, and merchant point-of-sale terminals. EBT cards are not immune as fraudsters use skimming technology to capture information such as the card number, personal identification number, and other information stored on the card. A fraudster can deploy a skimmer in a terminal in as little as seven seconds. The captured card information is then used to clone the victim's EBT card. Criminals will then cash out at the opportune time—usually when the card is loaded for the month. The legitimate recipient is left without food assistance for the next month, and American tax dollars are looted. Because cards are loaded monthly, the process is repetitive and predictable, creating a target rich environment for skimmers.

In one recent investigation, in collaboration with the U.S. Attorney's Office in the Eastern District of Louisiana, five Romanian nationals were indicted in a fraud scheme to steal nearly $1 million in SNAP benefits from low-income families by skimming. According to the indictment, the defendants allegedly conspired to install skimming devices onto legitimate card readers at retailers in Ohio and California. To carry out the SNAP benefits theft in Ohio, skimmers were mailed from California to several local locations in Ohio, then placed on point-of-sale devices at food retailers and gas stations. Defendants then checked card balances before draining the EBT accounts of their funds to load onto blank cards, which they then illegally re-sold.

These vulnerabilities in the SNAP payment system can also be a target for Federal Bureau of Investigation (FBI)-designated Transnational Organized Crime (TOC) groups. In one investigation in Louisiana, two Romanian nationals were indicted for access device fraud. According to court documents, the two individuals possessed device-making equipment, namely credit/debit card skimmers, at multiple locations. Both subjects are confirmed to be part of TOC groups. According to the FBI, TOC groups protect their activities through corruption, violence, and an organizational structure that spans national boundaries. These groups also engage in drug trafficking and human smuggling. Some groups use the illicit proceeds to fund other crimes, including, potentially, terrorism.

SNAP trafficking is also a serious concern for OIG. Today, there are more than 250,000 food retail stores authorized to exchange food for SNAP benefits, including popular grocery chains, big box retailers, convenience stores, and bodegas. These retailers participate in SNAP as an

important part of the distribution channel that supplies food to program recipients. When EBT cards are used at their stores to buy food, retailers then make claims for Federal reimbursement. Unscrupulous retailers will instead use their stores to launder SNAP benefits for cash. An individual will sell their EBT card, sometimes for pennies on the dollar in cash, and the retailer will extract the remaining value from the card or sell it.

Trafficking can also include exchanging SNAP benefits for other ineligible items like guns and drugs. In Operation "Mic Drop," USDA OIG special agents supported local and Federal law enforcement to investigate SNAP trafficking at a local store in southern California. Over $2 million was stolen from American taxpayers in the scheme. SNAP EBT benefits were exchanged with store employees for cash and then used to buy illicit drugs like crack cocaine from gang members located at the store. According to the San Diego District Attorney's Office, gang members used the money "to buy guns, which were used to perpetuate the cycle of violence." SNAP fraud enabled by corrupt retail stores can create a gateway for other violent crimes that can victimize entire communities by propping up a hub for criminality. OIG is committed to prevent SNAP benefits from funding gang activity and illegal drug purchases.

EBT terminal fraud is also a growing concern. State administrative agencies contract with third-party processors to facilitate Federal reimbursement to retailers that exchange food for SNAP benefits. To become authorized to receive SNAP, the USDA Food and Nutrition Administration (FNA) must determine that the store complies with program rules and issues a unique identifier. Terminal cloning, or processor fraud, describes the use of unauthorized terminals that allow fraudsters to impersonate an authorized retailer and direct SNAP payments to their own bank accounts. In a recently closed case from last year, a single terminal cloning scheme resulted in a $66 million loss. Shamefully, the theft was made possible by a USDA employee who betrayed her Oath of Office and sold FNA numbers to co-conspirators. That employee was sentenced in the Southern District of New York to 2 years in Federal prison. OIG will continue to pursue insider threats who abuse their public position for personal profit.

OIG's audit work is crucial to the fight against fraud by identifying the systems, processes and structural safeguards appropriate to prevent schemes, ensure proper payments and promote program integrity. For example, we recently determined whether FNA has taken actions to secure information technology hardware to effectively prevent SNAP benefit theft through card

skimming, card and terminal cloning, and other similar fraudulent methods. We found that FNA has taken steps to improve SNAP EBT security; however, FNA has not required States to adopt security standards to prevent SNAP benefit theft, resulting in $555 million in funds to be put to better use. We made one recommendation to FNA to develop a plan to issue regulations for States to implement SNAP EBT security measures. FNA agreed with our finding and is taking corrective action.

Deterring SNAP Fraud

Deterring fraud requires exacting real consequences on those that steal from taxpayers and the low-income Americans who qualify for SNAP assistance. OIG is steadfastly committed to investigating SNAP fraud and working with prosecutors to hold perpetrators to account. Since February 2025, OIG investigations have led to arrest of nearly 1,000 individuals; 133 convictions; and more than $135 million in restitution, fines, and assessments for SNAP-related violations. This remains one of OIG's top law enforcement priorities. We are proud of our partnerships with Federal, State, and local authorities to investigate allegations of fraud and our work with prosecutors to hold fraudsters to account.

Although a strong law enforcement response is critical, we cannot pay and chase our way to stopping SNAP fraud. To be effective, we need to guard the front door by ensuring that proper internal controls are in place to prevent fraudsters from infiltrating the system. Modern technology available to criminals makes it imperative that administering agencies at the State and Federal levels adopt appropriate modern technology and tools to verify an applicant's identity and other information provided before making payments. With the availability of online SNAP applications and internet food purchases, identity verification and authentication are critical to prevent fraud rather than chasing after criminals.

For example, earlier this year, in a case investigated by USDA OIG, the United States Attorney's Office for the District of Massachusetts charged three people, including two foreign nationals, for using the stolen personal information of over 100 real people from multiple States to fraudulently obtain $440,000 in SNAP benefits. In a different case, an Idaho jury convicted an individual for using the identity of a child from a different State who died in 1977 to obtain benefits from numerous Federal programs, including SNAP. These crimes took place across multiple States and persisted for a long period of time, revealing serious flaws in identity

verification. Verifying an applicant's identity and other information provided before making a payment would deter cases such as these.

In addition, we need to be sure that every part of the process is working together to create a hostile operating environment for any would-be fraudster. Distributing food to eligible SNAP recipients involves a patchwork of Federal, State, and local actors, third-party intermediaries, financial institutions, and more than 250,000 retail operations. Each link in this chain is a potential entry point for fraud. Moreover, enforcement is divided between Federal, State, and local agencies. Information silos and lack of coordination create openings for criminals to exploit.

Our ability to identify and prevent SNAP fraud would benefit tremendously from improved information sharing between the Federal Government and the States. Although USDA maintains data on authorized retailers, individual States maintain data on their own program participants. Access to this important information would allow Federal oversight to evaluate the effectiveness of internal controls at the applicant level and help fix vulnerabilities. For example, after Ohio shared participant data in response to our request, OIG auditors identified $13.3 million in data anomalies. With the results, before public release of our report, Ohio already began taking steps to address the findings. Our audit inspection and analytics work in Ohio is part of a series of engagements to assess the quality and integrity of SNAP participant data, with a focus on the information States use to validate participant eligibility. We chose the top 10 States for SNAP spending to conduct this inspection. OIG is still waiting for participant data from four States after requesting the information more than a year ago. Without the requested data, we cannot even begin to identify potential problems at the State level, much less make recommendations to improve them.

Withholding data from the watchdog Congress created to guard the front door not only obstructs essential Federal oversight, but it benefits fraudsters who steal from the individuals in their States who rely on USDA food assistance. Access to participant information across the program would allow more effective use of data analytics tools to identify fraud, such as duplicate enrollments and suspicious patterns. SNAP administering authorities need a common operating picture to connect the dots.

The convicted criminal that used the identity of a deceased child to get Federal benefits circumvented fraud controls across multiple Federal agencies over the course of 25 years. In OIG's experience, it is common for fraudsters to exploit more than one Federal assistance program in multiple jurisdictions. Access to comprehensive information about the use of Federal assistance programs by individuals across States and agencies will help administrators connect the dots before tax dollars are inappropriately paid out. Linking and leveraging detection and prevention systems across Federal and State agencies is a force multiplier against fraud. Greater access among agencies to each other's data is an important fraud prevention measure.

Low-tech security measures associated with SNAP are outmatched by hi-tech schemes. For example, almost all States continue to load benefits on magnetic strip cards, a decades-old technology that is far behind security measures of modern card payment systems. OIG recently completed an audit of the security of these EBT cards and recommended improvements. State and Federal SNAP administering agencies should evaluate and address potential security vulnerabilities across the system so there are no soft entry points for fraud. Fraud identification, detection, and prevention systems should be updated to meet the tactics of modern fraudsters.

Conclusion

In closing, I would like to thank the Members of the Subcommittee for your continuing interest in SNAP fraud and OIG's work to identify, detect, and prevent fraud. Your support enables OIG to continue ensuring SNAP runs as intended, confirming benefits reach intended recipients, stopping fraud, and bringing those to justice who seek to defraud the program.

This concludes my testimony. I would be pleased to answer any questions you may have.