



U.S. Department of Agriculture
Office of Inspector General

Review of Food and Nutrition Service Supplemental Nutrition Assistance Program/Electronic Benefits Transfer Hardware

January 2026

Inspection Report 27801-0001-12



Review of Food and Nutrition Service Supplemental Nutrition Assistance Program/Electronic Benefits Transfer Hardware

Inspection Report 27801-0001-12

FNS has taken steps to improve SNAP EBT security; however, FNS needs to strengthen controls related to SNAP EBT hardware as it 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.

OBJECTIVE

Our objective was to determine whether Food and Nutrition Service (FNS) has taken actions to secure IT hardware to effectively prevent Supplemental and Nutrition Assistance Program (SNAP) benefit theft through card skimming, card and terminal cloning, and other similar fraudulent methods.

BACKGROUND

The SNAP Electronic Benefits Transfer EBT is an electronic system that allows a participant to pay for food using SNAP benefits. These benefits are delivered to participants on a magnetic stripe debit card. Electronic Benefits Transfer systems, like debit and credit card purchases, use a point-of-sale to process SNAP transactions. SNAP Electronic Benefits Transfer fraud—such as card skimming and card cloning—to steal benefits is on the rise. Modernizing EBT, including the introduction of chip cards for SNAP Electronic Benefits Transfer, is an important step towards the protection of SNAP benefits.

REVIEWED

We reviewed and analyzed FNS' controls related to SNAP Electronic Benefits Transfer hardware to determine whether they were adequate to identify and prevent fraud schemes, such as card skimming and card cloning, between November 2024 and July 2025.

WHAT OIG FOUND

We found that Food and Nutrition Service (FNS) has not required States to adopt security standards to detect and prevent Supplemental Nutrition Assistance Program (SNAP) benefit theft. FNS stated this occurred due to the lengthy process to publish and codify a public rule. As a result, between October 2022 and December 2024, FNS replaced \$322 million in benefits likely due to fraudulent activity. Moreover, SNAP remains vulnerable to benefit theft; thus, in fiscal year 2025 and fiscal year 2026, the Office of Inspector General forecasts FNS may experience \$233 million in fraudulent activity. Combined, the \$555 million in SNAP benefits subject to fraudulent activities are funds to be put to better use.

WHAT OIG RECOMMENDS

We recommend that FNS develop a plan and timeline to issue regulations for States to implement SNAP Electronic Benefits Transfer security measures that detect and prevent card cloning and skimming fraud so that the projected fraudulent and replaced benefits, totaling \$555 million, could be put to better use.

FNS agreed with our finding, recommendation, and monetary result. We accepted management decision for the recommendation.



OFFICE OF INSPECTOR GENERAL

United States Department of Agriculture



DATE: January 15, 2026

INSPECTION

NUMBER: 27801-0001-12

TO: Patrick Penn
Acting Administrator
Food and Nutrition Service

ATTN: Amanda Musgrove
Director, Office of Internal Controls, Audits, and Investigations
Office of Financial Management
Food and Nutrition Service

FROM: Yaris Rivera-Rojas
Acting Assistant Inspector General for Audit

SUBJECT: Review of Food and Nutrition Service Supplemental Nutrition Assistance Program/Electronic Benefits Transfer Hardware

This report presents the results of our inspection of the Review of Food and Nutrition Service Supplemental Nutrition Assistance Program/Electronic Benefits Transfer Hardware. Your written response to the official draft is included in its entirety at the end of the report. Based on your written response, we are accepting management decision for the recommendation in the report, and no further response to this office is necessary.

In accordance with Departmental Regulation 1720-1, final action needs to be taken within 1 year of the date of each management decision. Please follow your internal agency procedures in forwarding final action correspondence to the Office of the Chief Financial Officer.

We appreciate the courtesies and cooperation extended to us by members of your staff during our fieldwork and subsequent discussions. This report contains publicly available information and will be posted in its entirety to our website (<https://usdaoig.oversight.gov>) in the near future.

Table of Contents

Background and Objective.....	1
Finding 1: FNS Has Not Required States to Adopt Security Standards to Protect SNAP Benefits	4
Recommendation 1	6
Scope and Methodology	8
Abbreviations	9
Exhibit A: Summary of Monetary Results	10
Exhibit B: Forecast Methodology	11
Agency’s Response	13

Background and Objective

Background

The Supplemental Nutrition Assistance Program (SNAP) Electronic Benefits Transfer (EBT) is an electronic system that allows a participant to pay for food using SNAP benefits. These benefits are delivered to participants on a magnetic stripe debit card. EBT systems, like debit and credit card purchases, use a point-of-sale (POS) to process SNAP transactions.

SNAP EBT fraud—such as card skimming and card cloning—to steal benefits is on the rise¹ (see the *Key Definitions* for terms related to SNAP and EBT fraud).

The magnetic stripe on payment cards is a common method for making payments with cards, but it is highly vulnerable to card cloning fraud. Criminals can use card skimmers to copy sensitive information from card stripes and transfer this information to blank cards. According to the Federal Bureau of Investigation, card cloning fraud costs both United States consumers and financial institutions approximately \$1 billion each year.²

Modernizing EBT, including the introduction of chip cards for SNAP EBT, is an important step towards the protection of SNAP benefits.³ Chip cards are a more secure payment option that make it more difficult for fraudsters to copy and steal SNAP account information, reducing the effectiveness of common fraud schemes.⁴

Preventing Fraudulent Attacks

Microchips (chips) play a crucial role in preventing card skimming and cloning. Chips are effective at countering counterfeit fraud because of tokenization, which replaces sensitive data—in this case the credit card's primary account number—with a token. When inserted or tapped over a chip-enabled terminal, the chip creates a one-time code to process the transaction. This dynamic makes it significantly harder for fraudsters to clone the card, as the transaction code

KEY DEFINITIONS:

SNAP EBT Fraud

SNAP EBT fraud occurs when individuals take advantage of SNAP participants for personal gain through fraudulent methods such as card skimming and card cloning.

Card Skimming

Card skimming is the unauthorized capture and transfer of payment data to another source for fraudulent purposes. A card skimmer is a device that criminals attach to POS machines to steal card numbers and other information from EBT cards. Most skimming attacks involve the capture of payment data from magnetic-stripe payment cards (non-chip cards).

Card Cloning

SNAP EBT card cloning occurs when the information from a legitimate card is copied onto a counterfeit card. This allows fraudsters to make unauthorized transactions using the cloned card, often without the cardholder's knowledge. The process typically involves capturing the card's magnetic stripe data and, in some cases, the personal identification number (PIN).

¹ USDA FNS, *SNAP EBT Modernization* <https://www.fns.usda.gov/snap/ebt/modernization> (last visited Aug. 18, 2025).

² Federal Bureau of Investigation, *How We Can Help You Scams and Safety* <https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/skimming> (last visited Aug. 18, 2025).

³ USDA FNS, *SNAP EBT Modernization* <https://www.fns.usda.gov/snap/ebt/modernization> (last visited Aug. 18, 2025).

⁴ Ibid.

cannot be reused. As such, the Office of Inspector General (OIG) believes chip cards are a critical control to mitigate current SNAP fraud transaction schemes.

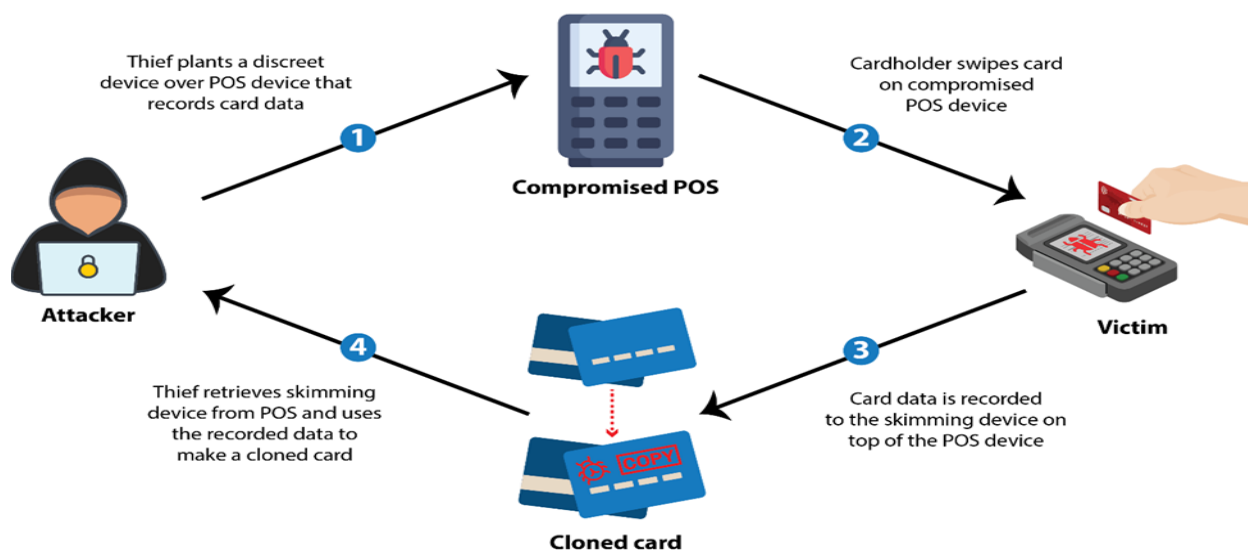


Figure 1: How card skimming fraud works. Figure by OIG.

Proposed Data Security Efforts

Food and Nutrition Service (FNS) has interim efforts underway to address terminal fraud schemes, such as:

- drafting a proposed rule to require State agencies to implement new card security measures and the publication of standards for States to implement chip-on-card technology; and
- following industry standards, such as The Payment Card Industry Data Security Standard (PCI DSS) through the publication of the X9.58 EBT standards (the standard) to significantly decrease the opportunity for fraud.

The PCI DSS is a set of security standards, designed by major credit card companies, to protect sensitive payment card information from fraud and data breaches. The PCI DSS consists of a four-part framework to protect sensitive data.

1. Fraud Prevention – Strategies to detect and prevent fraudulent activities.
2. Security Standards – A comprehensive set of rules to protect card holder data.
3. Compliance – Ensuring adherence to regulations to avoid penalties.
4. Data Protection – Measures to safeguard information from unauthorized access.

Additionally, the Accredited Standards Committee, in conjunction with FNS, developed the standard to help combat fraud associated with the current magnetic stripe EBT cards. The standard establishes requirements for SNAP terminals including:

- ☑ Provides technical specifications for exchanging financial transaction messages between the acquirer and EBT card issuer.
- ☑ Specifies message structure, format and content, and data elements and values used in SNAP.
- ☑ Provides increased security to lower instances of benefit fraud.
- ☑ Mirrors the existing security requirements for vendors that currently accept chip cards.

Objective

Our objective was to determine whether Food and Nutrition Service (FNS) has taken actions to secure IT hardware to effectively prevent Supplemental and Nutrition Assistance Program (SNAP) benefit theft through card skimming, card and terminal cloning, and other similar fraudulent methods.

Finding 1: FNS Has Not Required States to Adopt Security Standards to Protect SNAP Benefits

We found that FNS has not required States to adopt security standards to detect and prevent SNAP benefit theft. FNS stated this occurred due to the lengthy process to publish and codify a public rule. As a result, between October 2022 and December 2024, FNS was required⁵ to replace \$322 million in benefits likely due to fraudulent activity. Moreover, SNAP remains vulnerable to benefit theft; thus, in FY 2025 and FY 2026, OIG forecasts FNS may experience \$233 million in fraudulent activity.⁶ The \$555 million in SNAP benefits subject to fraudulent activities are funds to be put to better use.



7 United States Code (U.S.C.) § 2016a states that the Secretary of the U.S. Department of Agriculture is responsible for promulgating regulations that require State agencies to improve security measures and issuing guidance to State agencies that describes security measures that:

- are effective in detecting and preventing theft of benefits, including card skimming and card cloning; and
- are consistent with industry standards.

FNS Actions to Address SNAP EBT Fraud

FNS issued guidance to States that describe security measures effective in preventing theft of benefits. The goal of these efforts is to shift SNAP from relying on less secure magnetic stripe technology to more secure technology used by U.S. credit and debit card issuers. The shift aims to enhance consumer protection and reduce benefit fraud. FNS has partnered with various States to pilot potential solutions. For more details, see Figure 2, which illustrates the efforts taken by FNS and the States to secure SNAP benefits.

Since 2023, FNS has engaged with States and industry partners through an independent governing body called the Accredited Standards Committee X9.⁷ The purpose of this collaboration is to align SNAP EBT technology with standards used in the credit and debit industry.

In August 2024, the X9 Committee published the revised standard⁸ that States should implement. The standards are intended to enhance the equipment used in food retail stores. By issuing the standards, FNS complied with the requirement outlined in 7 U.S.C. § 2016a to issue guidance.

⁵ U.S. House of Representatives, *Office of the Law Revision Counsel United States Code* [7 USC 2016a: EBT benefit fraud prevention](#).

⁶ Per 7 U.S.C. 2016a, the replacement of benefits was approved for benefits stolen between October 1, 2022, and ending on December 24, 2024. FNS is no longer authorized to replace stolen benefits with Federal funds.

⁷ Accredited Standards Committee X9 Inc., [Overview of X9 - Accredited Standards Committee X9](#) (last visited June 2, 2025).

⁸ This standard provides all parties involved in EBT processing for SNAP and Cash benefit programs with technical specifications for exchanging financial transaction messages between an Acquirer and an EBT card issuer processor.

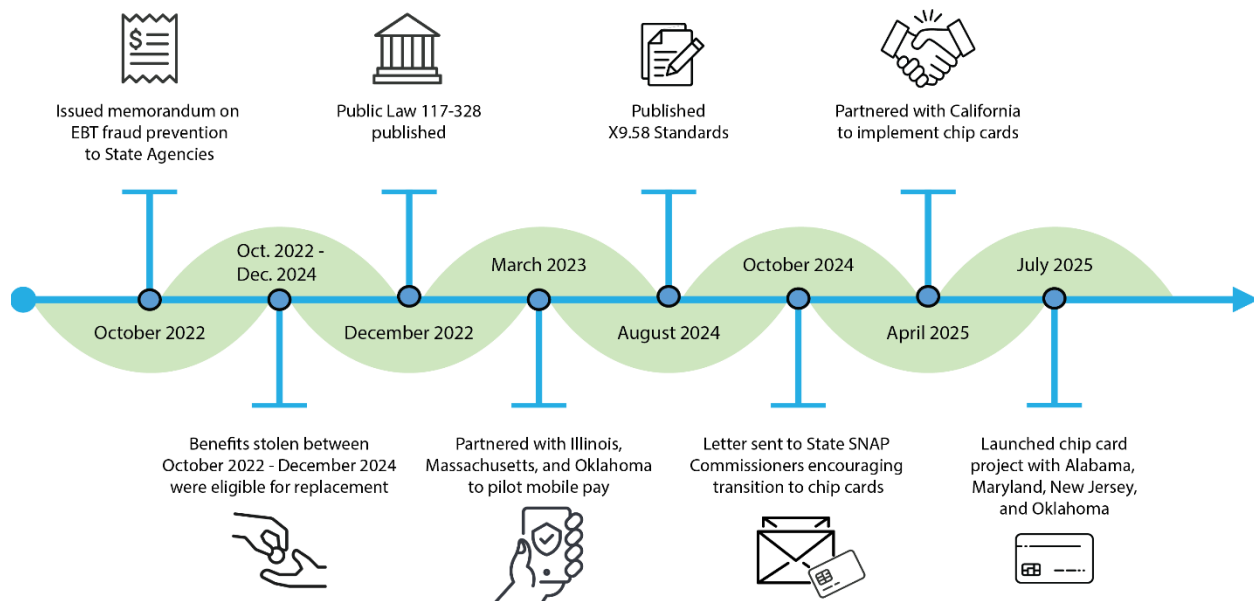


Figure 2: Timeline of actions taken by FNS related to SNAP EBT fraud. Figure by OIG.

Regulations to Prevent Theft of Benefits

Although FNS issued guidance to States describing security measures that can be implemented to detect and prevent benefit theft, FNS has not issued regulations that require States to implement the security measures. In the Spring of 2024, FNS began developing a new rule to formally incorporate the revised SNAP EBT standards into regulation and establish timelines for States to upgrade to these secure payment technologies to prevent the theft of benefits. However, as of August 2025, FNS stated the rule remained in draft form due to the lengthy process to codify a new rule. Theft of SNAP benefits is an ongoing Nationwide crisis,⁹ impacting both individuals who rely on these benefits and taxpayers who fund the program. FNS has reported on SNAP EBT theft driven by schemes such as card skimming and card cloning. The Consolidated Appropriations Act of 2023 included provisions for the replacement of stolen EBT benefits with Federal funds between October 1, 2022, and December 20, 2024.

Based on the historical data of replaced stolen benefits reported by the States, as depicted in Figure 3 below, we forecasted the future value of benefits losses over the next two FYs (FY 2025 and FY 2026) based on a statistical analysis.¹⁰ The analysis was derived from data provided by 53 States and territories, encompassing the period from October 2022 to December 2024. The data indicates that if FNS does not implement and enforce stronger security measures, such as chip cards, the projected loss from fraudulent activity over the next 2 years could exceed \$233

⁹ Every day, SNAP benefits are electronically stolen from EBT accounts all over the country and States are no longer receiving Federal funds to assist with the replacement of stolen benefits. SNAP/EBT Fraud, [South Carolina Department of Social Services](#) (last visited Aug. 5, 2025).

¹⁰ This analysis is based on the following assumptions: (1) historical stolen rate trends are predictive of future behavior; (2) program growth and inflation are captured by the compound annual growth rate applied to benefit costs; (3) no significant policy changes (such as technology, fraud detection, chip cards, mobile payments, etc.); and (4) each State's historical data quality is consistent and representative.

million. This projected loss, combined with the previously replaced benefits, would amount to \$555 million. OIG determined these as funds to be put to better use if controls over the SNAP cards are not improved¹¹ (see Exhibit B for calculation details).

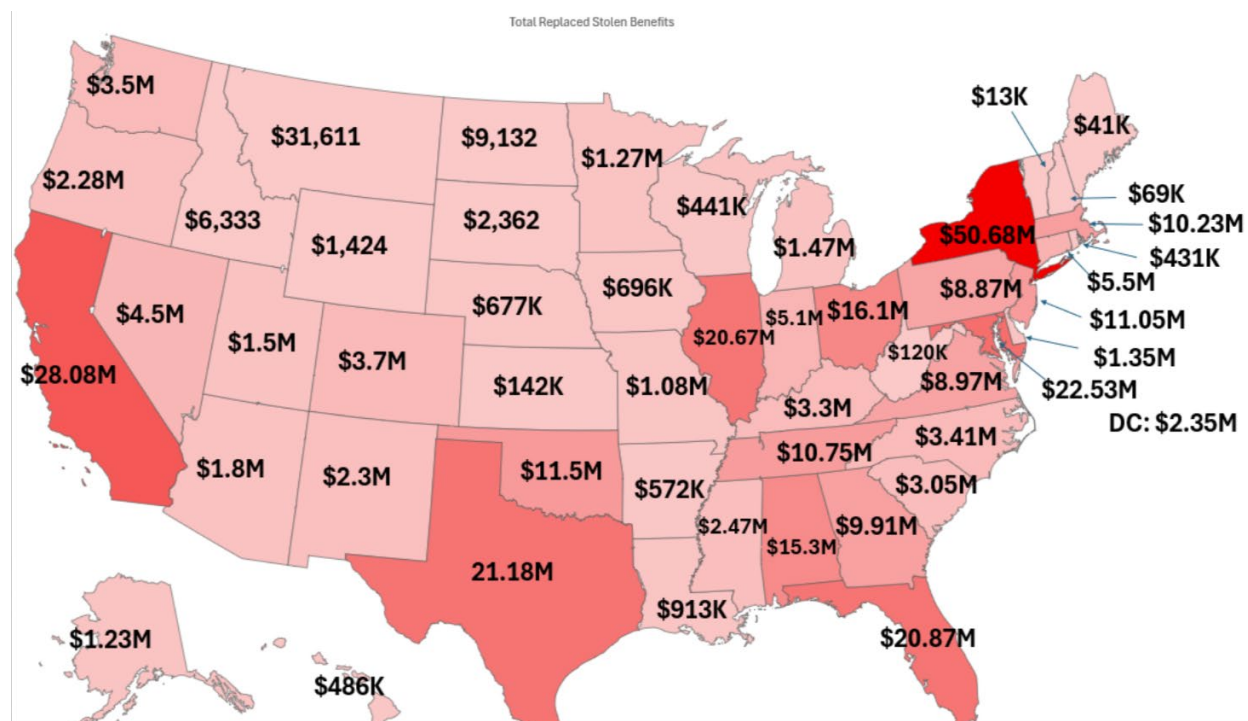


Figure 3: Total replaced benefits reported by States and Territories, between October 1, 2022, and December 20, 2024. Figure by OIG.

Recommendation 1

Develop a plan and timeline to issue regulations for States to implement SNAP Electronic Benefits Transfer security measures that detect and prevent card cloning and skimming fraud so that the projected fraudulent and replaced benefits, totaling \$555 million, could be put to better use.

Agency Response

FNS agreed with the recommendation and monetary result. FNS noted it has taken steps to draft a proposed integrity rule that will include language to increase SNAP EBT security measures, thereby decreasing card skimming and cloning and other similar fraudulent means. FNS could not replicate OIG's forecasted total. However, FNS

¹¹ The total amount of funds to be put to better use includes \$322 million of benefits replaced between October 2022 to December 2024 and \$233 million forecasted by OIG.

generally agreed that SNAP benefits were stolen through electronic benefit theft in 2025 and 2026.

FNS anticipates that the proposed integrity rule will be published by September 30, 2026.

OIG Position

We accept management decision for this recommendation. For Final Action, FNS needs to provide the Office of the Chief Financial Officer with a copy of the published integrity rule described in the agency's response.

Scope and Methodology

The scope of our inspection covered the security controls and information technology hardware of FNS' SNAP EBT cards and terminals. We conducted our fieldwork between November 2024 and July 2025. We reviewed FNS' controls related to SNAP EBT hardware to determine whether they were adequate to effectively identify, prevent, and deter fraud schemes such as card skimming, card and terminal cloning, and other similar fraudulent methods. Additionally, we reviewed FNS' program enhancements related to EBT security along with implementation strategies to determine whether they were aligned with industry standards and best practices.

We utilized the OIG Office of Analytics and Innovation to forecast the potential future value of SNAP stolen and replaced benefits across U.S. States and territories (see Exhibit B). These forecasts were based on historical SNAP stolen benefits claims data and SNAP participation data from October 2022 and December 2024. We obtained documentation to ensure these specialists were qualified professionally, competent in the work we relied upon, and met independence standards.

We did not independently review or assess the agency's information system(s); therefore, we make no representation regarding the adequacy of the agency's computer system(s), or the information generated from it.

To accomplish our objective, we:

- Interviewed FNS SNAP program personnel;
- Examined documentation related to statutorily required security enhancements;
- Assessed Department and agency policies and procedures around SNAP program oversight;
- Reviewed requirements of public law and regulations;
- Obtained and reviewed guidance and correspondence between FNS and State agencies, Congress, and governors; and
- Reviewed FNS' compliance with industry best practices related to card security.

We discussed the results of our inspection with FNS officials on December 2, 2025, and included their comment as appropriate.

The inspection was conducted in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*.

Abbreviations

CAGR	Compound Annual Growth Rate
chips	microchips
EBT	Electronic Benefits Transfer
FNS	Food and Nutrition Service
FY	fiscal year
IT	information technology
OIG	Office of Inspector General
PCI DSS	Payment Card Industry Data Security Standard
PIN	personal identification number
POS	point-of-sale
SNAP	Supplemental Nutrition Assistance Program
the standard	X9.58 EBT standards
U.S.C.	United States Code
USDA	U.S. Department of Agriculture

Exhibit A: Summary of Monetary Results

Exhibit A summarizes the monetary results for our inspection report by finding and recommendation number.

Finding	Recommendation	Description	Amount	Category
1	1	Replaced Stolen Benefits and Projected Future Fraudulent Activity	\$555,915,262	Funds to be Put to Better Use
Total			\$555,915,262	

Exhibit B: Forecast Methodology

We calculated a projection of SNAP replacement benefit costs for FYs 2025 and 2026 and determined these costs as funds to be put to better use.

A ratio-based forecasting method was applied. The key steps include:

Step 1: Calculate Replacement Ratios

For each State, calculate the replacement ratio as a percentage of total benefit costs.

1. Sum benefits costs over 27 months (per State)
2. For each State:
 - Replacement Ratio = (Total Value of Replaced Benefits over 27 months) ÷ (Total Benefit Costs over 27 months)

This ratio indicates the proportion of replacement per benefit dollar.

Step 2: Calculate SNAP Benefit Costs Compound Annual Growth Rate (CAGR)

Calculate CAGR¹² over the last three FYs (FY 2022 to FY 2024) to use in forecasting future years' benefit costs.

Step 3: Forecast Future Benefit Costs (FY 2025 to FY 2026)

For each future year FY 2025 to FY 2026, forecast benefit costs as:

$$\text{Forecasted_Benefit_Cost_FY}_n = \text{FY2024 Benefit Cost} \times (1 + \text{CAGR})^{n-2024}$$

Where n = FY (2025 to 2026)

Step 4: Apply Replacement Ratio to Forecasted Benefits

For each State and each FY (FY 2025 to FY 2026):

- Forecasted Replacement Benefits = Forecasted Benefit Cost × Replacement Ratio

Assumptions

- Replacement ratios remain stable relative to benefit cost over time.
- Program growth and inflation are captured by the CAGR applied to benefit costs.
- Each State's 27-month historical data is consistent and representative.
- No significant policy changes (such as technology and fraud detection) drastically alter the stolen rate.

¹² Using FY 2022 to FY 2024 data from [SNAP Data Tables | Food and Nutrition Service](#) (last visited Aug. 6, 2025).

Limitations

- No Seasonality or Trend Adjustments: Monthly or quarterly variation is not captured.
- Static Ratios: State-specific changes in enforcement or fraud risk are not incorporated.
- Uniform Growth Rate: Assumes a consistent CAGR across all States, which may overlook regional variation.
- Simplified Approach: Does not incorporate behavioral, demographic, or systemic modeling elements.

**Food and Nutrition Service
Response to Inspection Report**



U.S. DEPARTMENT OF AGRICULTURE

Date: December 31, 2025

To: Yaris Rivera-Rojas
Acting Assistant Inspector General for Audit

From: Patrick Penn /s/

Acting Administrator
Food and Nutrition Service

Deputy Undersecretary
Food, Nutrition, and Consumer Services

Subject: OIG Inspection 27801-0001-12, Review of Food and Nutrition Service Supplemental Nutrition Assistance Program/Electronic Benefits Transfer Hardware

This letter responds to the official draft report issued on December 11, 2025, for inspection number 27801-0001-12, Review of Food and Nutrition Service (FNS) Supplemental Nutrition Assistance Program (SNAP)/Electronic Benefits Transfer (EBT) Hardware. Specifically, FNS is responding to the one recommendation made to the agency in the report.

If you have any questions or need additional information regarding this response, please contact Amanda Musgrove, Director of the FNS Office of Internal Controls, Audits, and Investigations (OICAI) at (703)305-2092 or Amanda.Musgrove@usda.gov.

OIG Recommendation 1

Develop a plan and timeline to issue regulations for States to implement SNAP EBT security measures that detect and prevent card cloning and skimming fraud so that the projected fraudulent and replaced benefits, totaling \$555 million, could be put to better use.

FNS Response

Agree with recommendation: X Yes No

FNS has taken steps to draft a proposed integrity rule that will include language to increase SNAP EBT security measures, thereby decreasing card skimming and cloning and other similar fraudulent means. FNS has stood up a SNAP Data Analytics Team to review State data to provide integrity oversight and assist in determining fraudulent patterns across the program.

Agree with monetary results: X Yes No N/A

Based on the methodology and figures that OIG provided for agency review and comment, FNS could not replicate OIG's forecasted total. However, FNS generally agrees that SNAP benefits were stolen through electronic benefit theft in 2025 and 2026.

Estimated Completion Date

FNS anticipates that the proposed integrity rule will be published by September 30, 2026.

Learn more about USDA OIG at <https://usdaoig.oversight.gov>

Find us on LinkedIn: [US Department of Agriculture OIG](#)

Find us on X: [@OIGUSDA](#)

Report suspected wrongdoing in USDA programs:



<https://usdaoig.oversight.gov/resources/hotline-information>

U.S. Department of Agriculture (USDA) is an equal opportunity provider, employer, and lender.

In accordance with Federal civil rights law and USDA civil rights regulations and policies, USDA, its Agencies, offices, and employees, and institutions participating in or administering USDA programs and operations are prohibited from discriminating based on race, color, national origin, age, disability, sex, religion, retaliation for engaging in protected civil rights activity or opposition to any practice made unlawful under any Federal antidiscrimination laws, or receipt of income derived from programs or activities conducted or funded by OIG, political beliefs, or marital, familial or parental status (not all bases apply to all programs). Remedies and complaint filing deadlines vary by program or incident. Persons with disabilities who require alternative means of communication for program information (e.g., Braille, large print, audiotape, American Sign Language, etc.) should contact the responsible Agency or USDA's TARGET Center at (202) 720-2600 (voice and TTY) or contact USDA through the Federal Relay Service at (800) 877-8339. Additionally, program information may be made available in languages other than English.

To file a program discrimination complaint, complete the USDA Program Discrimination Complaint Form, AD-3027, found online at [How to File a Program Discrimination Complaint](#) and at any USDA office or write a letter addressed to USDA and provide in the letter all of the information requested in the form. To request a copy of the complaint form, call (866) 632-9992. Submit your completed form or letter to USDA by (1) mail: U.S. Department of Agriculture, Office of the Assistant Secretary for Civil Rights, 1400 Independence Avenue, SW, Washington, D.C. 20250 9410; (2) fax: (202) 690-7442; or (3) email: program.intake@usda.gov.

Cover photos are from USDA Flickr and are in the public domain. They do not depict any particular audit, inspection, or investigation.

