ATARC

DEMONSTRATING ROI IN SNAP THROUGH THE EBT CARD / CHIP CARD USE CASE

ATARC Fraud Detection and Mitigation Working Group | September 2026

TABLE OF CONTENTS

Acknowledgements: 2

I. Purpose, Audience, and Format 3

II. Problem Statement: Persistent Cost and Inefficiency in SNAP Delivery 3

III. The SNAP Card: Current Model and Controls 6

IV. Proposed Enhancement: Chip-Enabled EBT and Strengthened Rules 7

V. ROI Framework for Fraud-Fighting Investments 8

VI. Quantifying Benefits: Illustrative SNAP ROI Story 10

VII. Barriers, Tradeoffs, and Enablers 12

VIII. Policy and Governance Implications 14

IX. Conclusion and Call to Action 15

Acknowledgments:

- Eric Rivera, Export-Import Bank of the United States (EXIM), ATARC Fraud Detection and Mitigation Working Group Government Chair
- Bobby Duffy, nForce AI, ATARC Fraud Detection and Mitigation Working Group Advisor Chair
- Tiffany Goddard, Carahsoft, ATARC Fraud Detection and Mitigation Working Group Carahsoft Chair
- Loay Oweis, ID.me
- Rebecca Shea, U.S. Government Accountability Office (GAO)
- Nicholas Weeks, U.S. Government Accountability Office (GAO)
- Latesha Love-Grayer, U.S. Government Accountability Office (GAO)
- Dennis Sendros, Centers for Medicare & Medicaid Services (CMS)
- Ferdous Khan, Federal Emergency Management Agency (FEMA)

Disclaimer: This document was prepared by members of the ATARC Fraud Detection and Mitigation Working Group in their personal capacities. The views and opinions expressed herein are those of the authors and do not necessarily reflect the official policy or position of any individual organization, employer, agency, or affiliated entity. This document is released for public use and distribution. It may be shared, cited, and reproduced without restriction, provided it is not used for commercial advertising, marketing, or product endorsement purposes. Nothing in this document should be construed as an endorsement of any specific technology, vendor, product, or service.

SNAP fraud has doubled in monthly case rates since 2024. Each dollar stolen now costs agencies $4.14 once administrative, investigative, and reputational expenses are included, up from $3.93 the prior year. [1]

This paper focuses on transaction fraud: EBT card skimming, cloning, and unauthorized account access. It makes the investment case for chip-enabled EBT cards and stronger point-of-sale controls. Application fraud (identity misrepresentation, eligibility fraud, and cross-state duplicate enrollment) is equally important and is treated here as a complementary investment. A complete program integrity strategy must secure both the card and the identity behind it. [2]

I. PURPOSE, AUDIENCE, AND FORMAT

Q: Who is this white paper intended for?

Federal and state SNAP and other benefit program leaders, OIGs and the audit community, IT oversight bodies, state/local oversight organizations, fraud/identity/AI working groups, and policymakers.

Q: What is the purpose of this white paper?

To show how investments in SNAP card security—specifically chip-enabled cards and smarter transaction controls—can measurably reduce fraud and administrative burden without cutting off legitimate access to benefits.

II. PROBLEM STATEMENT: PERSISTENT COST AND INEFFICIENCY IN SNAP DELIVERY

Q: What legacy vulnerabilities exist in the current SNAP EBT system?

Magnetic-stripe EBT cards are vulnerable to skimming, cloning, and organized fraud. Fragmented state systems and vendor contracts cause widely varying security controls across the country.

Q: How significant and persistent is the fraud problem?

Fraud has persisted despite continuous efforts to combat the problem with improved controls and monitoring. Direct losses are only part of the impact: investigations, card reissuance, and customer support all contribute to major operational costs.

[1] LexisNexis Risk Solutions, True Cost of Fraud Study: SNAP (September 2025).

[2] Some states address this through the Public Assistance Reporting Information System (PARIS), an ACF-administered federal–state match that detects duplicate benefits across programs, including SNAP. All 50 states, D.C., and Puerto Rico can participate, but participation is inconsistent.

Q: What is the core tension in SNAP program goals?

SNAP administrators face a familiar squeeze: deliver benefits quickly, but also stop fraud. Tighter controls carry a real risk of disrupting benefit access for vulnerable households. Vendors also resist absorbing that cost (see “What drives vendor resistance,” below).

Q: Which states have already issued chip-enabled EBT cards?

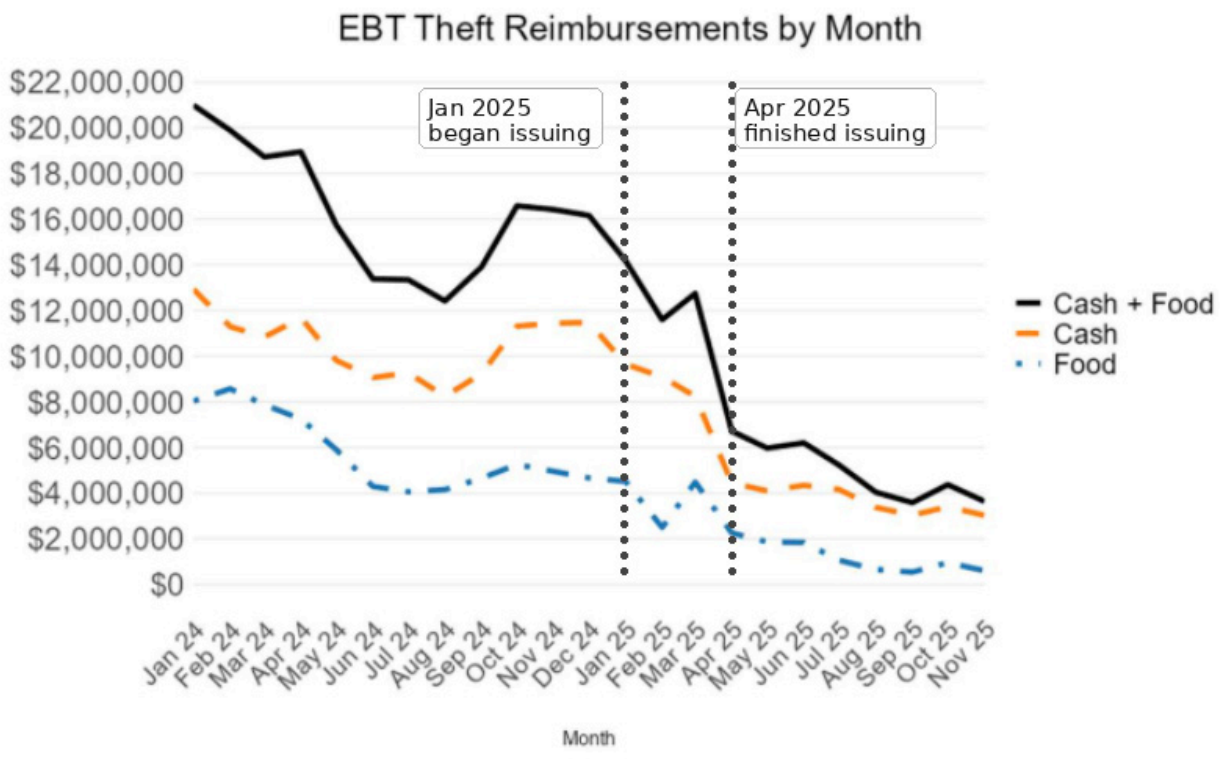
California and Alabama are notable examples though other states such as New Jersey have also issued EBT chip cards. Other states such as Oregon and Arkansas have EBT chip card projects in progress. Worth noting: when states upgrade, fraud networks have shifted activity to neighboring states that haven’t, which makes the case for coordinated adoption over a patchwork rollout. USDA tracks EBT modernization at SNAP EBT Modernization.

Q: Have chip-enabled EBT cards been successful at reducing fraud?

SNAP administrators face a familiar squeeze: deliver benefits quickly, but also stop fraud. Tighter controls carry a real risk of disrupting benefit access for vulnerable households. Vendors also resist absorbing that cost (see “What drives vendor resistance,” below).

Yes. California’s pilot in early 2025 and statewide rollout (Feb–Apr 2025) corresponded with a big drop in monthly EBT theft from $16.16M (Dec 2024) to ~$3.58M (Sept 2025)—a 78% decrease. Chip technology was a major factor, among several other improvements.

The graph below shows the decline in EBT theft alongside card issuance milestones. [3] [4]



[3] California reduces theft of food and cash benefits by 83% with state-of-the-art technology

[4] Electronic Benefit Transfer Theft and Updates on Implementation of Prior Funding Investments Report to the Legislature

Q: Are there challenges reaching specific vulnerable populations, such as unhoused individuals?

Yes. Getting updated cards to unhoused individuals is harder than standard mail delivery and state outreach strategies vary.

Q: Does EBT card fraud only happen at the point of sale, or does fraud also occur upstream at enrollment?

No. Card skimming and cloning occur at the transaction stage, but fraudulent account creation such as through synthetic identities, duplicate enrollments across states, and ineligible applicants is another problem. Chip cards handle transaction-level fraud; they do nothing about someone who obtained a fraudulent account before ever using the card. Addressing one without the other leaves the program only partially protected.

Q: How prevalent is duplicate enrollment or "double-dipping" across state lines?

Fragmented state systems without a shared identity layer allow individuals to claim benefits in multiple states simultaneously. [5]

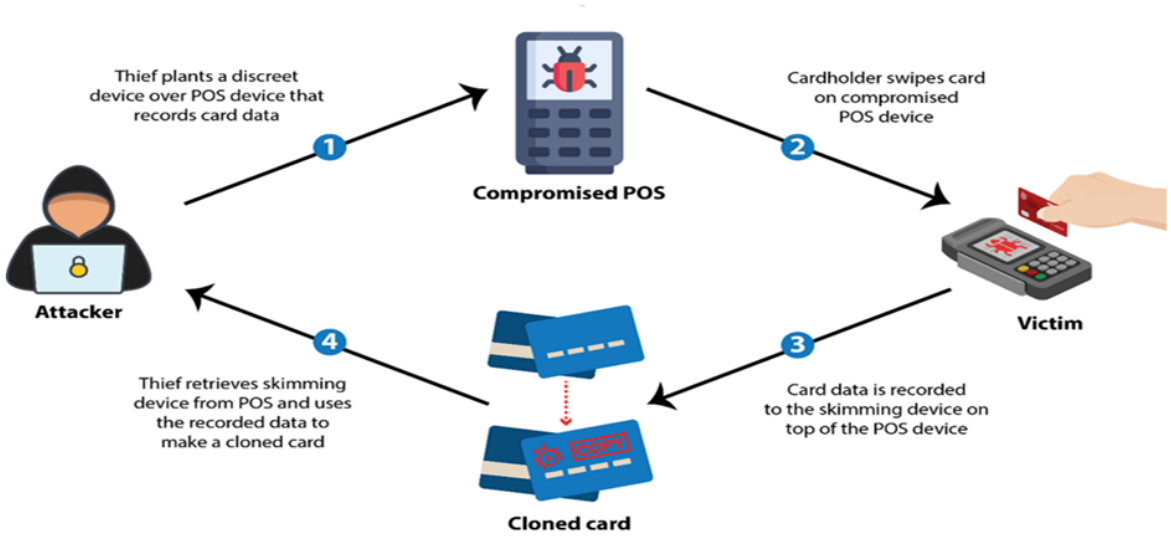
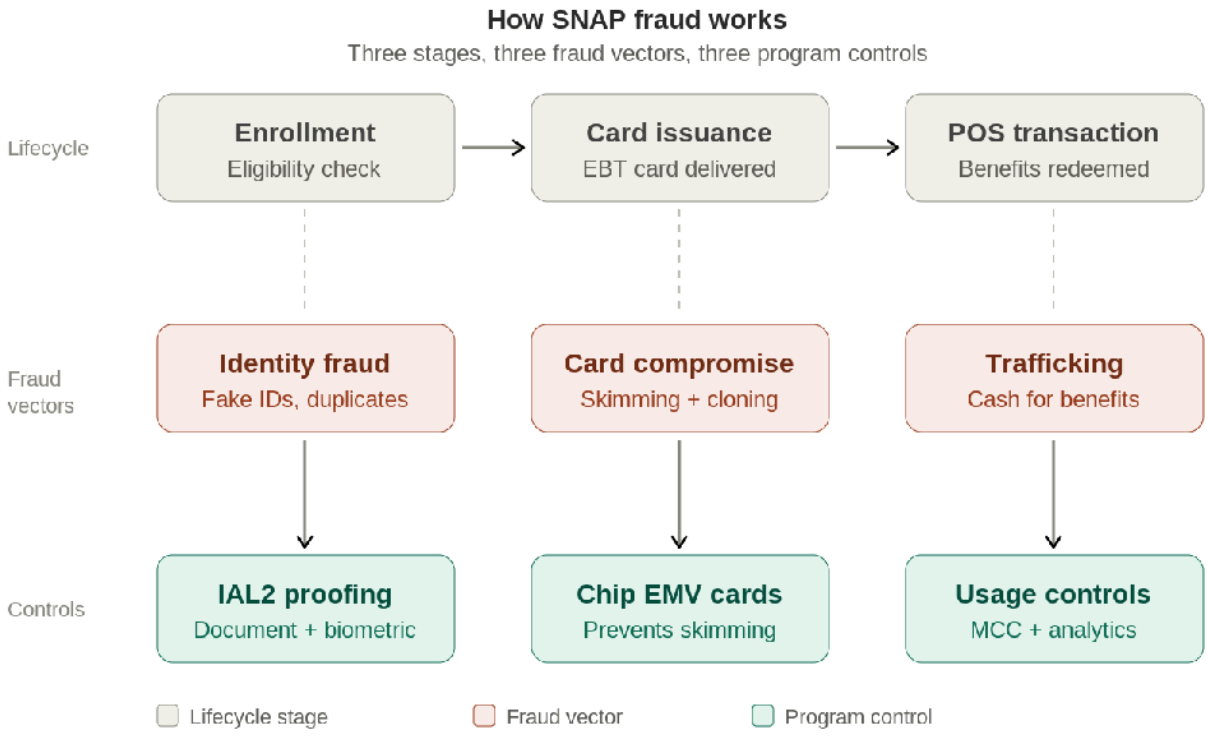


Figure 1: How card skimming fraud works. Figure by OIG.

Source: USDA OIG Inspection Report 27801-0001-12, Review of Food and Nutrition Service Supplemental Nutrition Assistance Program/ Electronic Benefits Transfer Hardware, issued in January 2026.

[5] Some states address this through the Public Assistance Reporting Information System (PARIS), an ACF-administered federal–state match that detects duplicate benefits across programs, including SNAP. All 50 states, D.C., and Puerto Rico can participate, but participation is inconsistent.

III. THE SNAP CARD: CURRENT MODEL AND CONTROLS



Q: How does the current SNAP EBT model work?

Beneficiaries use an electronic card tied to their benefit account at approved retailers. Controls include PINs and transaction rules enforced by state agencies and their vendors.

Q: What restrictions currently govern SNAP card use?

Cards cannot be used for alcohol, tobacco, or hot prepared foods. Some states also implement merchant category code (MCC) restrictions and limits on online purchases. SNAP Food Restriction Waivers that restrict the purchase of non-nutritious items like soda and candy.

Q: What are the key gaps and inconsistencies in the current system?

State-specific rules create uneven protection. Organized fraud networks know these weaknesses and exploit them. There's no consistent national data on the type and scale of specific attack scenarios that could be used to help combat fraud.

IV. PROPOSED ENHANCEMENT: CHIP-ENABLED EBT AND STRENGTHENED RULES

Q: How do chip-enabled EBT cards reduce fraud?

They prevent skimming and cloning by generating a unique transaction code for each purchase similar to credit and debit cards.



Source: GAO-25-107964, titled *"Nutrition Assistance: USDA Should Comprehensively Assess Benefit Theft Prevention Measures States Are Implementing"*, released September 25, 2025

Q: What complementary controls should accompany chip cards?

Strengthened and standardized MCC restrictions, analytics-based monitoring of online and abnormal transactions, and clear division of responsibility between states and vendors should accompany chip cards.

Q: What is the current state of chip EBT adoption?

California and Alabama are piloting or deploying chip-enabled EBT. USDA and OIG have started documenting and reporting on these transitions publicly. Pilot data and lessons from these states will provide important data for other states to consider.

Q: Are retailer point-of-sale (POS) systems a barrier to chip adoption?

Yes. Not all retailer systems are chip-ready. Costs and upgrade responsibilities are important constraints that must be considered in any implementation plan.

Q: What is the role of single-audit findings in this context?

Persistent findings in single audits can provide useful insights into potential fraud risks. Unfortunately, these audits have not been effectively leveraged. They are not consistently performed across states, their findings have often gone unaddressed, and trends in findings are not used to target risk management. This leads to a system with accountability and oversight gaps where fraud can operate freely.

Q: How does identity verification at enrollment complement chip-card security at point of sale?

Chip cards secure the transaction at the point of sale while identity proofing at enrollment (document verification, biometric matching, liveness detection) determines who initially gets an account. Both controls are necessary. Chip cards address post-enrollment fraud, and identity proofing stops fraudulent accounts from being created at all.

Q: What identity assurance standards apply to federal benefit programs?

NIST SP 800-63 Identity Assurance Level 2 (IAL2) requires remote or in-person identity proofing with document verification and biometric matching and is the standard used across many federal civilian programs. Applying IAL2 to SNAP enrollment or re-certification could significantly reduce the rate of synthetic identity and eligibility fraud.

Q: Can AI-generated documents or deepfakes defeat current identity verification controls?

Yes. Fraudsters are already using AI-generated IDs and deepfake video to defeat document verification and selfie-match checks. Modern identity verification systems need liveness detection and AI-trained fraud models to keep up.

V. ROI FRAMEWORK FOR FRAUD-FIGHTING INVESTMENTS

Q: How is ROI defined in a public sector context?

Public sector ROI should consider program integrity and public value. ROI calculations should include financial returns (losses prevented, detected, and recovered), operational returns (reduced administrative burden), and harder-to-quantify returns like public trust and continuity of access for legitimate beneficiaries.

Q: What counts as a fraud-fighting investment (the cost side)?

Technology and system enhancements (transaction monitoring, identity verification), investigative and enforcement staffing, administrative and compliance overhead, participant-facing controls and verification processes, and the cost of measuring and reporting outcomes. The potential impact on beneficiaries should also be considered.

Q: What counts as a return (the benefit side)?

California and Alabama are piloting or deploying chip-enabled EBT. USDA and OIG have started documenting and reporting on these transitions publicly. Pilot data and lessons from these states will provide important data for other states to consider.

Q: Are retailer point-of-sale (POS) systems a barrier to chip adoption?

Financial returns are fraud losses prevented, detected, and recovered. Operational returns include reduced administrative burden. Non-financial returns include program integrity, public trust, and continuity of access. Not every benefit can be monetized, and benefit calculations should also consider factors that can't be easily monetized.

Q: How should fraud deterrence be measured?

Deterrence is hard to measure because it attempts to account for fraud that wasn't attempted. Practical approaches include pre/post comparisons, regression analysis, and benchmarking against comparable states or programs. Deterrence impacts are worth considering.

Q: What are the key KPI dimensions for measuring ROI?

The framework covers six areas:

- **Fraud Losses Prevented:** Value of fraudulent transactions stopped before completion; estimated reduction in fraud losses before and after the enhancement; long-term cost avoidance.
- **Fraud Losses Detected:** Number and value of fraud incidents identified; changes in case size and frequency; intelligence value for internal controls; timeliness of detection.
- **Fraud Losses Recovered:** Dollar value recovered from detected fraud. True recovery rates as a share of detected losses are typically small.
- **Operational Efficiency:** Reduction in investigative hours, call-center volume, card reissuances, and staff time on eligibility and fraud casework.
- **Program Integrity and Public Trust:** Effect on legislative and stakeholder confidence, reduction in negative press coverage, impact on funding sustainability and political support, auditability.
- **Program Participant Experience:** Continuity of access for legitimate beneficiaries, speed of resolution for fraud-related holds.

Q: How should ROI be measured for identity verification at enrollment vs. card security at point of sale?

Card security ROI is measured primarily by reductions in skimming and cloning incidents and associated losses. Enrollment identity verification ROI is measured by reductions in fraudulent accounts created, duplicate enrollments detected, and ineligible payments made before detection. Track both separately, then combine for a full program integrity picture.

Q: What data and information sources are available to draw from?

- USDA/OIG reports on SNAP and EBT system vulnerabilities: U.S. Department of Agriculture Office of Inspector General
- Industry and research reports (e.g., LexisNexis) on fraud cost multipliers
- GAO: Combating Fraud: Approaches to Evaluate Effectiveness and Demonstrate Integrity
- International Public Sector Fraud Forum (IPSFF) Fraud Loss Measurement Framework
- California's data-driven benefit theft reduction (83% reduction reported in January 2026)
- USDA: Nutrition Assistance: USDA Should Comprehensively Assess Benefit Theft Prevention Measures
- USDA: *The Extent of Trafficking in SNAP: 2015–2017*
- State ROI reports on PARIS duplicate benefits reduction: PARIS Project Can Help States Reduce Improper Benefit Payments

VI. QUANTIFYING BENEFITS: ILLUSTRATIVE SNAP ROI STORY

Q: Which states can serve as reference models?

California and Alabama are early adopters and the most useful references at this time. California reduced food and cash benefit theft by 83% using chip and tap technology (reported January 2026). FY 2025 SNAP Fraud Framework Grant Awards are another source.

Q: What are the short-term, tangible impacts of chip EBT investment?

Fewer fraudulent transactions go through. Card replacement and customer support costs drop. The volume of manual investigations into skimming and cloning falls.

Q: What are the longer-term, strategic benefits?

Organized fraud networks are less effective against chip infrastructure. Transaction data quality also improves, supporting analytics including AI-driven monitoring. Better data also helps policymakers make better decisions about the program, including potential future integrity actions.

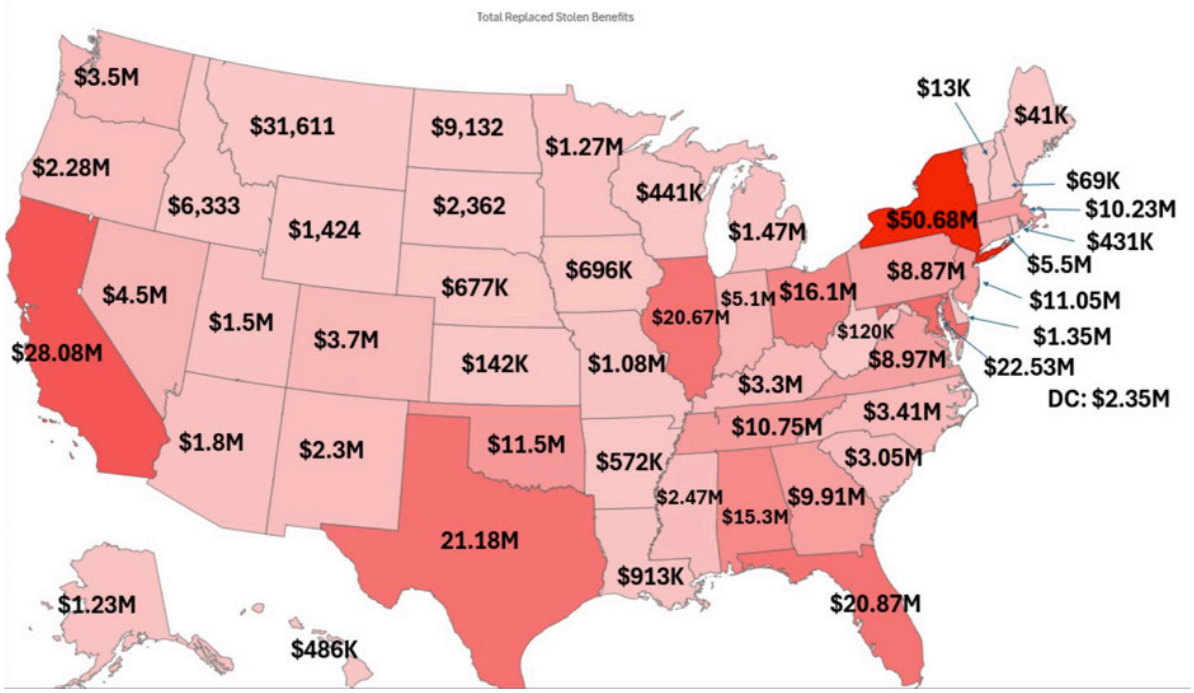


Figure 3: Total replaced benefits reported by States and Territories, between October 1, 2022, and December 20, 2024. Figure by OIG.

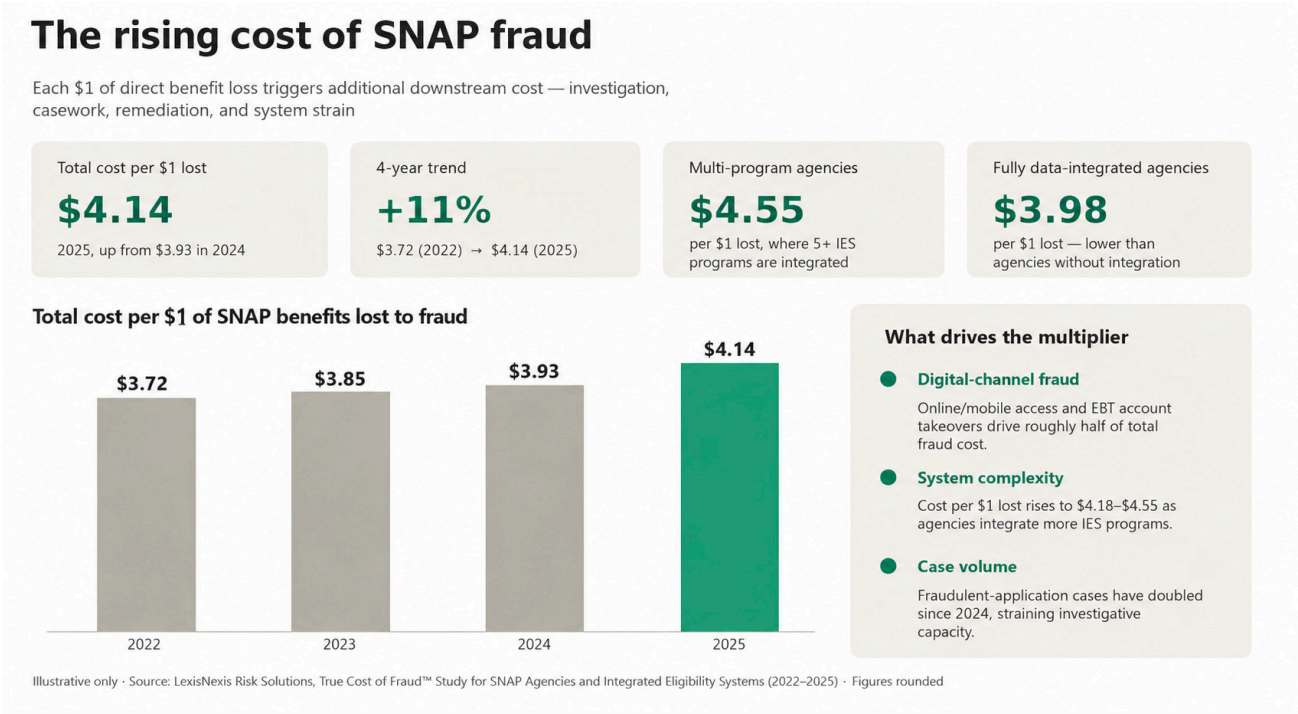
Source: USDA OIG Inspection Report 27801-0001-12, Review of Food and Nutrition Service Supplemental Nutrition Assistance Program/ Electronic Benefits Transfer Hardware, issued on January 2026.

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 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 improved.

Q: Can you provide an illustrative ROI scenario?

If a jurisdiction invests $X in chip cards and enhanced controls and conservatively reduces fraud incidents by Z% over N years, the avoided benefit payouts plus administrative savings can exceed the initial investment by [X+Y]. Assumptions must be transparent and figures tailored to real, jurisdiction-specific data. The goal is a story others can adapt, not a one-size-fits-all number.

Illustrative Example, California-Calibrated Scenario: A state with 500,000 SNAP households experiencing $50M in annual EBT theft invests approximately $15–20M to deploy chip-enabled EBT cards statewide. Applying California's observed 78% reduction in card-compromise fraud, the state could conservatively prevent $35–39M in theft annually. Within 12–18 months, avoided fraud losses exceed the upfront investment, before accounting for reduced card reissuance costs (approximately $5–10 per card), lower call-center volume, and fewer investigative staff hours. Under this scenario, the 5-year direct ROI exceeds 4:1, rising further when deterrence and administrative savings are included. Note: these figures are illustrative; jurisdictions should model against their own theft baselines, card stock costs, and vendor contract terms.



VII. BARRIERS, TRADEOFFS, AND ENABLERS

Q: What is the difference between SNAP improper payments and fraud?

Improper payments and fraud are distinct concepts. Improper payments can have fraud-related root causes and impacts, but not all are caused by fraud. Improper payments cover any payment made in the wrong amount, to the wrong recipient, or for an ineligible purpose, including administrative errors, unintentional overpayments, and failures to catch eligibility changes. Fraud requires intentional misrepresentation or deception. SNAP's FY2024 improper payment rate was about 11.5%, representing roughly $10.9B out of approximately $95B in annual benefits. The majority of those have been attributed to eligibility determination errors and documentation gaps, not willful fraud. Card skimming and retailer trafficking are examples of willful fraud. A caseworker missing an income change is typically an improper payment. ROI frameworks and policy interventions need to treat these separately because the controls that address each are distinct.

Q: What is the scale of individual beneficiary fraud in SNAP?

SNAP serves about 41 million individuals across roughly 22 million households. The program's annual improper payment estimate of approximately $10.9B (FY2024, USDA/OMB) is the broadest measure of payment integrity risk, covering both fraud and administrative error. Benefit theft directly affecting recipients (cards skimmed and benefits drained without the cardholder's knowledge) is a distinct and growing subcategory and USDA OIG data shows states replaced hundreds of millions in stolen benefits in recent fiscal years. [6] Duplicate enrollment across state lines, made possible by fragmented state systems without a shared identity layer, is a separate fraud vector that's difficult to quantify nationally but has shown up in OIG audits as a persistent gap. Chip cards address transaction-level theft while IAL2-level identity proofing at enrollment addresses fraudulent account creation. Both safeguards are required to combat fraud.

Q: What is the scale of retailer trafficking losses in SNAP?

Retailer trafficking is where authorized SNAP retailers exchange benefits for cash at a discount, or work with recipients to generate fraudulent transactions. USDA's most recent trafficking study (2015-2017) estimated annual losses at roughly $1.3B across about 260,000 authorized retailers. Unlike skimming, which chip cards directly address, stopping retailer trafficking requires merchant-side controls such as analytics-driven transaction monitoring, MCC restrictions, and targeted enforcement against high-risk retailers. The ROI framework should track different fraud vectors separately, since they require different investments and produce different measurable outcomes.

[6] Food and Nutrition Service's Supplemental Nutrition Assistance Program Fraud Risk Assessments

Q: How might stronger card security controls affect SNAP participation?

More friction at enrollment or point of sale carries a genuine risk of reducing participation among eligible households, particularly unhoused individuals who may not get mail for card delivery, elderly applicants who aren't comfortable with chip-and-PIN interfaces, and communities with limited access to updated POS terminals. Implementation plans need real outreach, transition support, and accessible alternatives (in-person card pickup, multilingual activation instructions). The access-versus-integrity tradeoff is real. Security improvements that lock out eligible beneficiaries undermine the program's purpose and create political and legal exposure.

Q: What financial and procurement barriers exist?

Upfront costs of replacing card stock and renegotiating vendor contracts are significant. Some agencies' budget rules classify security enhancements as overhead rather than investments, which makes them harder to fund through standard channels.

Q: What operational and stakeholder challenges exist?

Coordinating change across states, vendors, and retailers is complex. Maintaining program access through the transition isn't optional (see the access-versus-integrity tradeoff above).

Q: What drives vendor resistance to more secure card technologies?

Cost is the major driver. Vendors that prefer lower-cost magnetic-stripe options don't have incentives to absorb chip-card infrastructure costs. Public-private collaboration with financial sector partners, who've already solved this problem in commercial payments, is a viable path forward.

Q: How can these barriers be overcome?

Pilot programs can prove value and surface design problems before a broader rollout. Clear communications and training help states and beneficiaries navigate the transition. Cross-government communities such as fraud working groups, GAO frameworks, and PRAC examples provide tested models. The pattern that works proof of concept, then prototype, then scale.

Q: Does stronger identity verification create access barriers for vulnerable SNAP populations?

This is the main equity concern. Populations without standard government-issued IDs, including unhoused individuals, elderly applicants, and some immigrant communities, may struggle with document-based identity proofing. Any identity verification layer needs alternative pathways (trusted referee models, in-person verification options) to avoid excluding eligible beneficiaries. The access-versus-integrity tradeoff needs to be addressed explicitly in design and policy, not assumed away.

Q: What privacy frameworks govern the use of biometric data in federal benefit verification?

Biometric data, such as selfie images used for liveness checks, is subject to federal privacy laws and agency-specific policies. Agencies need clear data retention, use limitation, and deletion policies. Applicants need to understand how their data is used and stored. That's both a legal requirement and a public trust issue.

VIII. POLICY AND GOVERNANCE IMPLICATIONS

Q: What federal policy changes are needed to ensure all states adopt chip-enabled EBT cards?

USDA/FNS has authority to set EBT card security standards as a condition of program participation, and the direction of OIG recommendations, GAO findings, and pilot state results points toward a federal mandate. Key policy options:

- FNS rulemaking to require chip-enabled (EMV) EBT card issuance and EMV-capable POS infrastructure as a baseline standard for all state SNAP programs, with a phased compliance timeline: 24-36 months for card stock replacement, 48 months for full POS readiness.
- Congressional appropriations or targeted FNS grants to offset state and vendor transition costs, framed as program integrity investments with measurable ROI benchmarks tied to demonstrated reductions in benefit theft.
- FNS coordination with payments industry partners and POS hardware vendors to ensure retailer readiness, particularly for smaller independent grocers who disproportionately serve
- SNAP communities and may not have capital to self-fund upgrades.
  Standardized national reporting requirements for EBT theft and fraud losses, enabling cross-state benchmarking and longitudinal ROI measurement as chip adoption scales nationally.

A coordinated national mandate is needed to prevent the neighbor-state effect, where fraud networks shift activity to adjacent states that haven't upgraded yet. California's 78% reduction in theft is a proof point. A patchwork of voluntary adoption won't get there at national scale.

Q: Why does ROI framing matter to decision-makers?

It moves the conversation from 'security vs. access' to 'smart investments that protect both.' It gives appropriators, oversight committees, and agency leadership the evidence-based framing they need to make and defend funding decisions.

Q: What broader policy frameworks does this connect to?

- SNAP Fraud Framework
- GAO's Fraud Risk Framework (especially the "evaluate and adapt" component, measuring and improving controls over time)
- GAO, A Framework for Managing Improper Payments in Emergency Assistance Programs (GAO-23-105876) — relevant because SNAP can be part of emergency assistance through the Disaster Supplemental Nutrition Assistance Program (D-SNAP), which provides temporary food benefits to people affected by a presidentially declared disaster.
- Payment Integrity Act and OMB guidance on fraud risk management

Q: How should state vs. federal roles be clarified?

Accountability questions, like the issues raised in cases such as Minneapolis, affect where investments and responsibility should sit. A visual mapping of state vs. federal roles in designing, funding, and overseeing SNAP card security is recommended as a companion piece.

IX. CONCLUSION AND CALL TO ACTION

Q: What is the core narrative shifting this white paper proposes?

Treat SNAP card security modernization, meaning chip-enabled cards plus smarter controls, as a strategic, data-backed investment rather than a discretionary cost.

Q: What specific actions are proposed for agencies and partners?

Assess current fraud and administrative cost baselines tied to EBT vulnerabilities. Engage with pilot states, auditors, and industry experts to sharpen the assumptions. Plan and fund incremental upgrades starting with pilots and measure outcomes rigorously.

