

7 Things You Need to Know About ...

EBT Fraud

A quick guide to understanding EBT Fraud from the



01 | WHAT IS IT?

Electronic Benefits Transfer (EBT) fraud refers to illegal schemes that steal or misuse government benefits delivered via electronic payment cards. These cards are used to access programs like SNAP (Supplemental Nutrition Assistance Program, formerly food stamps) and TANF (Temporary Assistance for Needy Families).

There are two main types of EBT fraud that affect the payments industry:



Card Compromise: Criminals skim EBT card data and PINs at point-of-sale terminals or ATMs, then clone the cards and extract funds before the fraud is detected. Because EBT cards use outdated magnetic stripe and PIN technology, they are especially vulnerable to card cloning and unauthorized use.



Trafficking/Refund: Fraudulent retailers collude with cardholders to “cash out” benefits. The retailer swipes the EBT card for a fake purchase and hands over cash, often pocketing a cut. When looked at in isolation, these transactions are often indistinguishable from legitimate ones.

EBT fraud is perpetrated by a mix of bad actors: dishonest merchants, complicit benefit recipients, and organized criminal networks.

Type	Contributor	Definition	Example
Recipient Misuse	Benefit recipients.	Using benefits in ways not allowed by the program.	Using SNAP benefits to buy non-food items or selling goods bought with EBT for cash.

02 | HOW DOES IT WORK

EBT fraud occurs when funds are issued for the intent to cash out to either a merchant or recipient for no true product in return.



Card Compromise: Card compromise can happen when EBT card skimmers are set up at legitimate markets and the EBT card information is then placed on a fake new card.



Fraudsters can create new EBT cards to use in criminal activities in two ways.

- Fraudsters can use the compromised cards at legitimate businesses to buy products.
- Fraudsters can use the compromised cards at unauthorized locations to obtain cash.



Fraudsters can either:

- Approach legitimate businesses to add a compromised FNS (Food Nutrition Services) number to their business in exchange for a portion of the funds.
- Submit a fraudulent credit card processing application that uses a compromised FNS number with the intent to deposit funds from that EBT card into their bank account.



EBT fraud deprives families who rely on government assistance of the funds allotted to them. The EBT recipients do not have any dispute rights.



Trafficking/Refund: In this type of fraud, the merchant is the victim and faces a potential loss. Fraudsters either steal a terminal from a business, have a terminal that accepts EBT, or colludes with an EBT-accepting merchant. They run refunds to cards they have access to (orphan refunds). The refunds debit the merchant and place funds on the fraudster's card. They typically spend those funds quickly on their fraud accounts with FNS#'s. The merchant is out the funds, and the fraudsters have been unduly enriched.



In some schemes, fraudsters conspire with EBT-accepting merchants to process fake transactions. The merchant withdraws the funds, passes a pre-arranged share back to the fraudster, and pockets the remainder.

Most of this fraud has to happen quickly because recipients are allotted new funds monthly.

03 | WHO IS DOING IT?

Type	Contributor	Definition	Example
Card Cloning and Skimming	Organized crime groups or tech-savvy criminals—often not the actual benefit recipients.	EBT card numbers and PINs are stolen through skimming devices and used to drain accounts.	A cloned EBT card is used to make unauthorized purchases.
Trafficking Fraud	Both the benefit recipient and a complicit store owner.	The illegal exchange of SNAP benefits for cash.	A recipient offers to "sell" \$100 in SNAP benefits to a store owner for \$50 in cash.
Retailer Fraud	Store owners and employees.	Authorized retailers commit fraud by running fake transactions or inflating prices to drain EBT cards.	A store charges an EBT card for \$200 of goods but gives only \$50 worth of items.

This APP publication is for general information purposes only. It does not constitute business or legal advice, and do not represent any undertaking to keep recipients advised as to any or all relevant industry or legal developments. Any information, views, or opinions expressed by contributors to this publication do not necessarily represent the views and opinions held by APP. APP assumes no liability or responsibility for the accuracy, completeness, or usefulness of any information presented in this publication.

04 | WHY IS IT SIGNIFICANT?

EBT fraud targets the most vulnerable members of society. Recipients don’t realize their funds have been stolen until they are standing at the register ready to purchase food for their family. Funds that are recovered from running “trafficking” transactions can also be used to fund illegal activity and it is difficult to track this type of activity.

Merchants who willingly collude with fraudsters and EBT card abusers are in danger of losing their ability to process these transactions and can even face criminal penalties from the U.S. government—as well as fines from the card brands.

Merchants who are victims of EBT fraud face reputational damage and potentially lose the ability to process EBT transactions.

Retailers	Play a critical role in larger-dollar fraud cases, often facilitating or initiating trafficking schemes.
Organized Crime Rings	Increasingly responsible for high-tech fraud (e.g., card cloning, mass skimming).

05 | WHAT IS THE DOWNSIDE?

The fallout from EBT fraud hits hard, especially for the most vulnerable, with ripple effects across society:



Massive Economic Drain:

EBT fraud siphons **\$4.7 billion annually** from public funds, per the U.S. Government Accountability Office (2024), equivalent to 3.8% of SNAP’s \$122 billion budget. This loss could provide 11.7 million monthly SNAP benefits (\$400 average for a family of four), leaving states scrambling to cover shortfalls and cutting into other welfare programs.



Widespread Victim Impact:

Over 1.2 million SNAP households were hit by EBT fraud in 2024, with losses totaling \$1.5 billion, per USDA data. In high-impact states like California, 1 in 10 EBT users reported theft, with 60% of victims facing food insecurity for 1-2 months while awaiting reimbursement, exacerbating hunger for 2.5 million individuals.

05 | WHAT IS THE DOWNSIDE? (continued)



Criminal Network Expansion:

EBT fraud fuels sophisticated crime syndicates, with 70% of 2024 cases linked to transnational groups, per the U.S. Secret Service. These networks, often involving over 500 operatives per ring, reinvest profits into other crimes like drug trafficking, costing law enforcement **\$150 million annually** to combat, diverting resources from local policing.



Economic Ripple Effects:

Fraudulent EBT transactions inflate costs for retailers and banks, with **\$200 million in chargeback** losses reported by merchants in 2024. This drives up prices for consumers, adding an estimated 0.3% to grocery inflation, which disproportionately burdens the 41.9 million SNAP-dependent Americans already stretched thin.



Long-Term Program Vulnerability:

Persistent fraud threatens SNAP's viability, with 2024 congressional reviews citing fraud as a reason to cut funding by \$10 billion over five years. This could reduce benefits for 5 million recipients by 15%, undermining a program that cut poverty rates by 8% for 12.8 million children in 2023, per the Census Bureau.

06 | WHERE IS IT GOING?

While fraudsters continue to find ways to be creative and steal EBT card benefits or find ways to collude with merchants, the payments industry and the government are working diligently to combat them.

Payment companies are working with new risk and monitoring systems to help detect potential fraud. The integration of artificial intelligence powered systems help analyze transactions patterns anomalies and suspicious activities. This includes flagging large EBT transactions, small test transactions, interstate EBT usage, and many other analytics.

The government recently introduced security chip enabled EBT cards to replace the original magnetic strip cards as well as legislation to help protect against EBT theft and fraud. The SKIM Act and the SNAP Anti-Theft and Victim Compensation Act are great examples of legislation.

These bills allow the U.S. Attorney General and the U.S. Department of Agriculture's Office of Inspector General to bring fraudsters to justice, while also deploying chip-protected cards to families/individuals who have been defrauded.

07 | WHAT ARE THE IMPLICATIONS FOR PAYMENTS?

EBT fraud poses significant challenges within the electronic payments ecosystem, particularly when government assistance programs like SNAP or TANF are exploited. Fraud in this space has cascading consequences for sponsor banks, acquirers, and ISOs, ranging from financial liability to reputational damage.

Sponsor banks' involvement in processing fraudulent EBT transactions can trigger regulatory investigations and audits. Agencies such as the USDA and DOJ may scrutinize their portfolios, and card networks like Visa and Mastercard could impose penalties or place the bank under monitoring programs. The bank's ability to sponsor acquiring services could be revoked altogether if the fraud is systemic or egregious.

Acquirers face similar risks. EBT fraud within their merchant base can tarnish the entire portfolio, exposing them to brand-imposed fines, chargebacks, and financial restitution requirements. These institutions may be compelled to tighten underwriting standards and enhance real-time fraud monitoring to protect themselves from downstream liability.

ISOs are often the weakest link when EBT fraud occurs, typically due to poor merchant onboarding or inadequate KYC practices. If an ISO is found to have knowingly or negligently facilitated EBT fraud, it may face termination by upstream processors, inclusion on the MATCH list, and a permanent loss of residuals.

To mitigate risk, all stakeholders must practice enhanced due diligence, monitor for anomalies in real time, and educate merchants on proper EBT use. Ultimately, a single act of EBT fraud can jeopardize an entire payments chain, making proactive risk management a compliance requirement and a business necessity.

This Seven Things publication was produced with contributions from members of APP's Strategic Interest Group on Fraud Trends.

Contributors

- James Filomena: Vice President of Sponsorship Oversight, Citizens Bank
- Jonathan Corona: COO, MobiusPay
- Bill Glass: COO, AltruPay
- Niamh Lewis: Vice President, G2 Risk Solutions
- Christine Harper: Director of Investigations, Global Payments
- Mark Creizman: Director of Risk & Compliance Advisory, Material Connections LLC
- Marlena Hubley, Principal, Rebeta Consultants LLC

About APP

The Association of Payment Professionals (APP) is a volunteer-driven, nonprofit, membership organization committed to safeguarding the payments ecosystem through education, collaboration, and leadership.