NEW YORK STATE OF OPPORTUNITY. | Office of Temporary and Disability Assistance

KATHY HOCHUL
Governor

DANIEL W. TIETZ
Commissioner

BARBARA C. GUINN
Executive Deputy Commissioner

General Information System (GIS) Message

Section 1

Transmittal:	22 TA/DC095 Upstate and New York City
Date:	October 19, 2022
To:	Subscribers
Suggested Distribution:	Commissioners, Deputy Commissioners, TA Directors, SNAP Directors, Staff Development Coordinators
From:	Valerie Figueroa, Deputy Commissioner Employment and Income Support Programs
Subject:	Skimming & Phishing: EBT Scams Currently Impacting Recipient Households
Effective Date:	Immediately
Contact Information:	Wendy DeMarco, Director of Food and Nutrition Programs, wendy.demarco@otda.ny.gov; Stephen Bach, Director of Program Integrity, stephen.bach@otda.ny.gov; Luke Posniewski, EBT Bureau Chief, luke.posniewski@otda.ny.gov/; Temporary Assistance Bureau at (518) 474-9344 or otda.sm.cees.tabureau@otda.ny.gov
Attachments:	Attachment 1: Safeguard Your Card Poster

Section 2

The purpose of this GIS message is to inform districts that the Office of Temporary and Disability Assistance (OTDA) has been made aware of increasing incidents of Temporary Assistance (TA) and Supplemental Nutrition Assistance Program (SNAP) benefits theft via several scams, and to increase TA/SNAP recipients' awareness of the risks posed by this ongoing criminal activity. This message will highlight the specific nature and methods of these scams and share information that can be used by households to help safeguard their benefits going forward.

Phishing Scam

This is not a new type of scam targeting Electronic Benefit Transfer (EBT) users, but it remains an effective method at stealing benefits. The entire recipient population should consider themselves at risk and be aware of their responsibility to safeguard their EBT card and personal identification number (PIN).

Generally, phishing scams appear as an official and legitimate email, SMS (text) message, or phone call that solicits confidential account information from an EBT household. These fraudulent messages will often direct the recipient to a third-party website or attempt to coax the recipient into providing their EBT card number and PIN, enabling scammers to create a point of access with which they may liquidate the victim’s benefit account balance.

Recently, phishing scams have employed deceptive tactics ranging from “smart tablet giveaways”, in which TA/SNAP benefit recipients are asked to submit personal case information to participate, to fraudulent requests for households to provide card and PIN information in order to access Pandemic Electronic Benefit Transfer (P-EBT) food benefits or to unlock an EBT account. OTDA will never send correspondence prompting a recipient to provide their account information.

Card Skimming

Card skimming scams directly copy card and PIN information from EBT users at legitimate retailers, using authorized EBT point of sale (POS) devices. This type of scam involves the use of a physical overlay device with Bluetooth technology to temporarily commandeer a retailer’s POS device. Once thieves have gained access to the POS device, they are able to steal (skim) and then remotely transmit card/PIN information to an offsite location. Typically, thieves then use this data to create a duplicate version of the card which then enables remote access to the compromised account.

Since skimming devices simply transmit information and otherwise allow legitimate EBT transactions to proceed unimpeded, targeted retailers and victims are typically unaware that theft has occurred until they have already been compromised. EBT account holders generally do not realize they have been victimized until their next attempted purchase or account balance review.

Although it is not immediately obvious to a household that their EBT account has been compromised, there are several steps that EBT cardholders can take to reduce risk and better safeguard their EBT cards from this type of theft:

- **Frequently Change EBT Account PIN**—Once a card has been skimmed, the duplicate card uses the same information stolen from the EBT user initially (e.g., card number and associated PIN). If the actual EBT cardholder changes their PIN, anyone attempting to gain access to the account via a duplicate card will be restricted because they will not have the updated information. It is recommended that cardholders avoid selecting a PIN that is easy to guess, such as repeated or consecutive numbers. For example, cardholders should avoid choosing a PIN of “2222” or “1234”.

- **Physically Inspect POS Devices**— Generally, a skimming overlay device (skimmer) is designed to look like the POS Device (card reading machine) that it is placed on top of. Once the overlay device covers the retailer’s card reading machine it will likely be indistinguishable to most onlookers. However, because the overlay device covers the entire faceplate of the card reading machine it will be larger than the original machine, so some physical signs might be noticeable. The signs will vary depending on the model of the retailer’s machine but given the size discrepancy between the original machine and the skimmer, the overlay device may obscure, block or cover certain features of the original card reading machine. For example, some recovered skimmer devices have been noted to block LED indicator lights, block the illumination of backlit keypad numbers, and misalign or partially cover stylus trays.

  Apart from these specific examples, there are also a number of more general signs that a skimmer might be in use. For instance, the faceplate of the card reading machine may be loose, appear ill-fitting, or be easily dislodged from the body of the machine. In some instances, the faceplate may be miscolored, texturally mismatched, or otherwise appear different than the body of the card reading machine. Please note that these physical signs are not an exhaustive list, nor are they meant to suggest that the presence of any single sign is definitively indicative of the presence of a skimming device, but rather provides households with some warning signs they should be aware of when using their EBT cards. Cardholders should always exercise caution when making purchases and refrain from using any card reading machine that they suspect may be compromised.

- **Report Suspicious Devices & Activity**— If an individual notices any signs that a skimmer may be in use, they should alert the retailer and refrain from using the possibly compromised machine. SNAP and TA households should regularly review their account transactions and balances and

immediately report their card lost or stolen should they identify any questionable activity or transactions. Clients may report their card lost or stolen at the EBT Customer Service Helpline (1-888-328-6399), on Internet at www.connectebt.com, on the **ConnectEBT** mobile app. When reporting the card lost or stolen using these methods, the client will also have the option to order a replacement card.

Program Implications

Theft of benefits due to phishing/skimming, is akin to any other theft of personal property or money, and recipients have the option to report this crime to their local police department.

SNAP
The United States Department of Agriculture, Food and Nutrition Service (USDA-FNS) prohibits replacing stolen SNAP benefits using federal funds. Additionally, stolen/skimmed SNAP benefits cannot be replaced even if a reported case of skimming is confirmed.

TA
TA benefits that have been stolen/skimmed, cannot be replaced, even if a reported case of skimming is confirmed. In addition, TA cannot be used to replace the amount of SNAP benefits stolen/skimmed.

Districts are able to issue an emergency food allowance, which would be under emergency assistance. The food allowance is limited to an amount not to exceed the sum of the basic allowance, HEA and SHEA, or restaurant allowance, if appropriate, for any given month. However, this is meant to be a last resort after households have explored all community resources. If a household refuses or does not utilize available resources to meet their food needs, they would not be eligible for an emergency food grant.

Required Action

The issue of skimmed EBT benefits is an increasingly prevalent problem nationwide. There are ongoing efforts by local, state, and federal law enforcement agencies to investigate and ultimately prosecute those responsible. Given this ongoing investigative effort, it is important that any instances of suspected or apparent digital benefit theft be referred to OTDA for review, confirmation and tracking.

Districts are being asked to assist in this effort by reviewing any reports of stolen benefits that appear to be examples of theft via skimming. Should a review of the EBT record reveal evidence that benefits may have been stolen through skimming, district staff must forward this information to Skimming@otda.ny.gov.

Clients should not be referred to make reports directly to this inbox*. *Only reports originating from district staff will be evaluated and tracked.

Please include the following information in all reports directed to this inbox:

- Client Name,
- Case number,
- CIN,
- Address,
- Phone Number,
- Total Amount Stolen,
- Whether it was Cash or SNAP,
- If the client has filed a police report

If households request a fair hearing due to scam-related stolen benefits, districts should contact their SNAP liaison or the TA Bureau (as appropriate) for further guidance.

Identifying Stolen Benefits

While it can generally be difficult to establish with absolute certainty if a benefit has been stolen via this skimming process, there are several obvious signs that districts should look for when reviewing the EBT transaction record. Typically, the fraudulent purchase transactions take place outside of New York State, and they liquidate the available balance of the EBT account (SNAP and/or Cash benefits) with either a single, large purchase transaction or several purchase transactions in a short window of time. The purchases will identify the user's card and Magnetic Stripe/Pin Entry as the transaction method, indicating that the purchase was made by swiping a card in person. These transactions have been observed to take place in a relatively short window of time following the client's legitimate purchase (at which point the card information was likely stolen). For example, the client may have made a legitimate, in-person purchase at a retailer in Long Island, and then an hour later several large, in-person purchases are recorded across multiple retailers in Texas.

The EBT transaction history will then likely show a balance inquiry or a 'denied: insufficient funds' transaction in the days following the theft – indicating the first time the EBT user typically becomes aware of the theft.

If any EBT theft is suspected, whether the physical card was stolen or the card was digitally compromised, the cardholder should immediately report the card as stolen and change their PIN.