LexisNexis®
RISK SOLUTIONS

Electronic Benefit Transfer (EBT) Card Skimming… A Deeper Look At The Issue

By Andrew McClenahan, Senior Director, Market Planning, LexisNexis Risk Solutions

Recent news articles related to fraud within public assistance programs—Supplemental Nutrition Assistance Program (SNAP), Temporary Assistance Nutrition Funding (TANF), Women, Infants and Children (WIC) —have focused on EBT Skimming. Food and Nutrition Services (FNS), Administration for Children and Family (ACF) and individual SNAP/TANF agencies have issued numerous client education materials aimed at informing genuinely needy and vulnerable participants on how to spot a card skimmer. Skimmers have historically and predominately been found on automated teller machine (ATM) and gas pumps targeting credit and debit cards. FICO saw a 368% increase in compromised cards in 2022.[1] So why are criminals suddenly targeting EBT devices? Or are they?

Account Take-Over (ATO) has been an issue for decades, as anyone who has had funds suddenly drained from a debit card knows. Credit card companies notify clients of suspicious transactions and monitor oversea purchases. Card skimming devices are but one tool in the arsenal of fraudsters looking to make an easy dollar. But now it's hitting the most vulnerable in society. Texas recently has directed recipients[2] to change their personal identification number (PIN) regularly and to freeze/unfreeze their card to prevent ATOs. California, long struggling with this issue, even provided numbers related to the depth of this problem: $84 million in anticipated 2023 losses… and that's just TANF (CalWorks).[3] Acknowledging that members of society will always be targets of phishing emails, texts, and phone calls, some of the other primary contributors to ATO (in no order) include:

Call Centers remain the number one target of opportunity for identity thieves as they can hide behind the anonymity of (spoofed) phone numbers to social engineer and scam call takers. Due to high call volumes, staff shortfalls, and the expense it takes to identify callers, operators continue to fall back on Name, Date of Birth (DOB), Social Security number (SSN), and a validating question (i.e., address, name of child on account). Unfortunately, every identity fraudster has this information on hand. Call centers remain a major vulnerability where clients (and fraudsters) can change account information, change addresses, order new cards, or reset PINs. Improving call center identity solutions and a federally mandated standard to states and EBT vendors is sorely needed. ***What is your state doing?***

Customer Service Portals have been critical in providing enhanced access to recipients to check balances, reset PINs, receive balance inquiries, or confirm when benefits will be loaded onto a card. Online portals lack sufficient safeguards to confirm the person accessing the portal is the client. Phone interactive voice responses (IVRs) commonly only require the last four digits of a SSN, a DOB, and sometimes a case number. Few states verify the phone number in the IVR. Even more rare is for state agencies to check for spoofed numbers, voice over internet protocols (VoIPs), or subscriber identity module (SIM) swaps. Technology and funding exist to stop these ATOs, so why have not states implemented these protections? ***The American Rescue Plan Act provided over $1 billion to states, $445 million this year[4]– funding exists to fix this.***

Online Identity Verification to verify legitimate recipients without requiring in-person applications presents the best opportunity to prevent synthetic identity fraud in the US banking system (projected $1.8 billion in 2020, and research suggests that the number could increase to US $2.42 billion in 2023[5]) to verify legitimate recipients without requiring in-person applications. This enhances equitable access. However, FNS current legal guidance is that states must allow applicants the option to opt-out of virtual identity protections and safeguards due to the antiquated name/address/signature requirements dating back to pen and paper. Best practices in the private sector can be used to authenticate identities without putting extra burdens on call centers. Identity data exists and should be used to protect the program. ***FNS must remove the opt-out guidance and require safeguards are in place to protect from fake applications, recertifications, or modifications that allow criminals access to legitimate accounts.***

Bot Attacks are on the rise as the Unemployment Insurance industry discovered during the Public Health Emergency (PHE). Transnational criminal groups and state sponsored terror groups were responsible for massive bot attacks, whether only several hundred a day, or millions as some states discovered. Without safeguards, scripts attacking states and county application sites were creating massive backlogs in requests for information, referrals to call centers, and delays in receiving benefits. And worse, the bot attacks are combining the tactics described above to create a fail-proof method of ATOs. ***Every state with an online portal or application must have bot-detection tools.***

Data Breaches/Dark Web continues to be a source of personal identifiable information (PII) needed to intercept legitimate client benefits. EBT cards—while statutorily considered credit cards—do not get the same benefit protections as a credit card. When breaches occur (ex. 2013 Target)[6], financial institutions issued new cards. No EBT cards were reissued, and most agencies do not monitor the Dark Web. Identity fraudsters can easily access PII to construct bot attacks, fraudulent applications, or breach client facing portals. ***States should utilize the power of digital identity/device data combined with physical identity data verifications used in the private sector.***

Fraudulent Retailers are complicit in multiple cases. While a device can be easily attached to an ATM or gas pump, skimming gadgets placed upon a point of sale (POS) machine in a small (high-risk) retailer are more difficult to later remove and present a greater risk to the bad guy. It is not just smaller businesses either. Bigger box stores are not actively monitored in FNS ALERT, so fraudsters can swipe multiple cards at checkout. Dishonest retailers have been an issue for decades; four years ago, the Government Accountability Office (GAO) declared SNAP trafficking estimates ranged from $1 billion to $4.7 billion[7]. ***Enhanced oversight and vetting in retailers are long overdue and can help stem the tide on ATOs.***

Third-Party Processors (TPP) distributing POS devices are no longer broadly apportioned or monitored by The United States Department of Agriculture (USDA) FNS. Their guidance relies on the retailers to vet the TPPs. TPPs have become the wild, wild west of the fintech world. The organized criminal fraternity has infiltrated this link in the EBT chain and have exploited the lack of oversight. POS devices lacking geolocation have resulted in devices being shipped to locations outside their operating area, including outside the country. A POS device only needs an internet connection (which can be spoofed to appear in the assigned area) while funds are drained by transnational criminals. ***Another reason why retailer integrity and rigorous background checks are the best preventative medicine.***

Cloned POS Devices are less frequent but still a contributing factor to ATOs. POS devices are cloned using legitimate retailer information but with altered bank routing information. What looks like a “big-box store” is actually a cloned POS device. Recipients trafficking benefits then have card and PIN information stored and stolen right after the next benefit upload. ***Stricter monitoring of transaction data is needed, but this also falls under “trafficking” issues already present.***

Card Tumbling is when criminals write computer scripts to produce EBT card numbers. They then brute force attack customer service portals and state/EBT/third-party applications. If a card exists, they reset the PIN and drain the account at a fraudulent retailer, online, or at mega stores. The main targets are states that use present personal identifiable number (PIN) numbers to standard formats (like using the last four digits of an SSN) or allow common PINs (i.e., 0000,1111,1234, etc.). ***Enhanced security on PINs and portals will help combat this tactic.***

LexisNexis®
RISK SOLUTIONS

Third Party Assistance is available online, whether it is additional eligibility services for SNAP applicants, or applications that can be downloaded and installed on smartphones. The offer of assistance or tools that require EBT card numbers, case numbers, PII, or PIN numbers may actually be identity fraud. Assistance is provided to applicants by States and/or counties at no cost. FNS just announced five states that will pilot a Mobile Payment Pilot as they search for ways to mitigate EBT card skimming. Photos and chips on cards may prevent some issues, but the trend towards smartphone wallets introduces new exposure that requires careful consideration and scrutinized lessons learned before a cardless pilot can be expanded. ***Again, robust identity verification solutions exist that can stop friendly/familial/authorized representative fraud attempts.***

This list is not exhaustive, and fraud trends can change weekly, daily, or even hourly. But as "Protectors of the Program(s)," we must educate our internal administrators and advocate for multi-layered solutions featuring advanced information and analytics that evolve with increasingly sophisticated fraud and skimming tactics. We cannot continue to expect our most vulnerable members of society to be responsible for spotting a skimming device. The issues are complex, but answers exist and are available.

Our commitment to the protection of these essential programs remains steadfast. Ensuring vulnerable people continue to receive the services they desperately need while maintaining program integrity and achieving a return on investment is critical – and obtainable. President Biden's State of the Union Address cited a 10:1 return on investment (ROI) in combatting fraud.[8] We look forward to the opportunity to partner with you as we achieve these goals.

LexisNexis® RISK SOLUTIONS

For more information:
Tel: 1-800-869-0751 or visit

1 US Card Skimming Grew Nearly 5x in 2022, New FICO Data Shows
2 HHSC warns of increased reports of SNAP, TANF recipients being targets of fraud | KXAN Austin
3 Card thieves target CalFresh, CalWORKs recipients- CalMatters
4 H.R.1319 - 117th Congress (2021-2022): American Rescue Plan Act of 2021 | Congress.gov | Library of Congress
5 Synthetic Identity Fraud: Diabolical Charge-Offs on the Rise | Aite-Novarica
6 https://www.commerce.senate.gov/services/files/24d3c229-4f2f-405d-b8db-a3a67f183883
7 https://banks.house.gov/uploadedfiles/fy23_budget_final_copy.pdf
8 https://www.whitehouse.gov/briefing-room/speeches-remarks/2023/02/07/remarks-of-president-joe-biden-state-of-the-union-address-as-prepared-for-delivery/