California Programs And Background

• TANF in California is known as “CalWORKs”
• SNAP in California is known as CalFresh
• State supervised, county administered benefit delivery system
• Each county operates a Special Investigative Unit (SIU) to prevent and pursue welfare fraud. These units may be part of the county welfare department or the district attorney’s office.
• The EBT vendor for California is FIS, since June 2018
Fraud Prevention Policy Framework

- **Client Fraud.** Individuals may deliberately misrepresent income, assets, or persons for the purpose of obtaining benefits for which they are not eligible.

- **Eligibility Worker Fraud.** Human services workers may inappropriately use knowledge or system access to wrongly issue benefits to themselves or accomplices.

- **Retailer Fraud.** Retail establishments may exchange cash for food benefits in deliberate violation of program rules.
What’s Missing? Third-Party Fraud

• The prevention of client, eligibility worker, and retailer fraud has been an aspect of public benefits administration for decades. Extensive state and federal guidance exists on these matters.

• However, the theft of benefits by those outside the system has not been a significant part of the welfare fraud prevention framework.

• Third Party Fraud: When outsiders steal benefits from clients or the system.
Two Examples of Third Party Fraud: Skimming and Scamming

• Skimming is the theft of electronic card data, including card number and PIN by sophisticated electronic surveillance.

• Scamming is the process of obtaining sufficient client personal information to enable a third party to reset an EBT card PIN and clone the card.

• Obtaining such information can be through trickery, via text or phone, and then falsely directing clients to a fake call center. It may also be obtained through other weaknesses in the system.
California Legislation

- Chapter 319, Statutes of 2012 (AB 2035, Bradford) authorized state reimbursement of TANF funds stolen by *skimming*. All County Letter (ACL) 13-67 provides guidance to counties and clients on how to file and process claims.

- Chapter 712, Statutes of 2018 (AB 2313, Stone) explicitly extended reimbursements to *scamming* cases, but limited such reimbursements to once in any three-year period. ACL 18-48 provides guidance on this process.

# Skimming and Scamming
Reimbursements, 2018-19, By Month

<table>
<thead>
<tr>
<th>Month</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jul-18</td>
<td>$9,110</td>
</tr>
<tr>
<td>Aug-18</td>
<td>8,050</td>
</tr>
<tr>
<td>Sep-18</td>
<td>8,913</td>
</tr>
<tr>
<td>Oct-18</td>
<td>9,281</td>
</tr>
<tr>
<td>Nov-18</td>
<td>27,693</td>
</tr>
<tr>
<td>Dec-18</td>
<td>36,980</td>
</tr>
<tr>
<td>Jan-19</td>
<td>31,841</td>
</tr>
<tr>
<td>Feb-19</td>
<td>60,635</td>
</tr>
<tr>
<td>Mar-19</td>
<td>39,701</td>
</tr>
<tr>
<td>Apr-19</td>
<td>47,874</td>
</tr>
<tr>
<td>May-19</td>
<td>25,039</td>
</tr>
<tr>
<td>Jun-19</td>
<td>13,713</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>$318,830</strong></td>
</tr>
</tbody>
</table>
Two EBT Third Party Fraud Cases

• Sonoma County

• Sacramento County

• Both cases correspond to the recent surge in EBT theft reimbursements
Sonoma County Case

• At a roll-over EBT call center, suspect employees apparently collected client case and EBT card information.
• Suspects used this information to clone cards, change PINs, and steal benefits.
• Initial suspects were identified through retailer surveillance footage.
• Cell phone search warrants resulted in more suspects comprising a ring of identity thieves operating near an Indian Casino.
• Cell phone data allowed state to see which EBT cards had been compromised.
• Five individuals arrested and charged with Grand Theft (2 call center employees, 2 boyfriends and one additional subject)
• Exact mode of theft remains under investigation
Still Learning About Sonoma Case

• Were there internal control weaknesses at the overflow call center?

• How did this fraud ring obtain full SSNs?

• Are there any lessons from this EBT call center that might apply to eligibility call centers?
Sacramento County EBT Theft Case

The Team:

• Lead Agency: Sacramento County Department of Human Assistance (SCDHA) Special Investigative Unit (SIU)

• Prosecution and Logistical Support: California Department of Justice (CDOJ)

• Data Analysis and Support for Data Sharing:
  • California Office of Systems Integration (OSI)
  • FIS Government Solutions (EBT vendor)
  • California Department of Social Services
What Does an EBT Scam Look like? Robo call or text “an alert”

"An alert concerning EBT card starting with 5077"

“Verification required for EBT renewal.”

Typically respondents instructed to provide:
- full EBT card number,
- PIN (associated with their EBT card),
- social security number, and
- date of birth

The automated response may sound very real to the client
Sacramento County Investigation

Criminal Investigators Burke and Fedor met with Sacramento County CalWORKs Program Specialist in early February 2019 to discuss recent claims for benefit theft reimbursement pursuant to the recently enacted AB 2313 legislation.

AB 2313 went into effect January 1, 2019, and it expands the protections for victims to those who have been scammed out of their EBT account information (no more than once every three years).

While determining how to best investigate potential fraud on the part of our clients, Sacramento County investigators looked into the reported theft transactions in Jan / Feb 2019.
EBT Robo Call victims

January and February 2019 – 10 cases reported Sacramento County
- Accounts accessed via Chase ATMs in Los Angeles after midnight, at the beginning of the month

What about other Chase EBT access after midnight, at the beginning of the month?
- November 2018 – April 2019
- Initially found 600 completed EBT transactions
- Almost $400,000 withdrawn, mostly between midnight and 6:00 a.m., immediately following cash benefit load on the first three days of the month
- 28 Chase Bank locations
- 2 Citibank
- 2 stand-alone ATM locations
Investigating the Phone Associated With the PIN Changes

- Sacramento County SIU worked with OSI and FIS to analyze the phone number used to change the PINs on these accounts.

- FIS developed an alert system to flag when this phone number contacted the EBT call center to reset the PIN

- This further enabled investigators to track the suspect.

- California DOJ worked with Sacramento County to establish surveillance in Los Angeles County where the suspect typically withdrew stolen funds in the early hours of the morning following the cash benefit load.
L.A. Operation: May 2019

May 1st early morning hours
- Suspect targeted five (5) locations
- Total of $22,325.00 from 48 different EBT accounts
- DOJ Team in L.A. were directed to the suspect’s location as he was withdrawing money in real-time (located suspect at 2 of the 5 locations)
- Mobile surveillance was unsuccessful, suspect was extremely elusive and perhaps aware of the surveillance
L.A.: May 2, Suspect Apprehended

FIS data streams
- 0103 withdrawal Reseda ATM
- 0149 withdrawal Canoga Park ATM
- 11 ATM transactions
- $9,115

Suspect arrested and found in possession of:
- $9,115
- 11 white plastic cards
- Toyota key
- Police scanner

What he did not have
- cell phone
- identification
- $$$ from Reseda ATM
May 14: The Car

Sac. SIU identified car registered to suspect Gibson

Found car just blocks from arrest site with ticket

<table>
<thead>
<tr>
<th>ITEM NUMBER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>001</td>
<td>US Currency - $3,992.55</td>
</tr>
<tr>
<td>002</td>
<td>US Currency - $5,550.00</td>
</tr>
<tr>
<td>003</td>
<td>One (1) Black Garmin GPS SN [redacted], with power cord</td>
</tr>
<tr>
<td>004</td>
<td>One (1) Black Wallet, containing CDL [redacted] (Jawuan Gibson), BoFATM Card [redacted], BoFA Acct. [redacted], Marriott Rewards card, 3 silver keys</td>
</tr>
<tr>
<td>005</td>
<td>One (1) Black Nexus Cell Phone model LG 0821</td>
</tr>
<tr>
<td>006</td>
<td>One (1) City of L.A. parking violation dated 5/7/19</td>
</tr>
<tr>
<td>007</td>
<td>One (1) Black backpack containing, 7 bundles of blank access cards with attached notes, one black beanie, one black Under Armor face mask, one pair of black sunglasses, one pair black gloves</td>
</tr>
</tbody>
</table>

Marriott Rewards Card (Hotel Key)
Finding The Hotel Room (May 14)

• The Marriott rewards care led investigators to the nearby Marriott, where the suspect has been staying for many months.

• After securing the room and obtaining a search warrant, investigators entered and found:
  • Multiple lap top computers
  • Multiple cell phones
  • A magnetic card stripe writer and reader
  • Sim cards, and blank plastic credit sized cards
  • Approximately $950,000 in cash
CA DOJ and the eCrime Unit (eCU)

The DOJ provided the surveillance and made the arrest in Los Angeles County.

The primary mission of the DOJ eCrime Unit is to investigate and prosecute multi-jurisdictional criminal organizations, networks, and groups that perpetrate identity theft crimes, use an electronic device or network to facilitate a crime, or commit a crime targeting an electronic device, network or intellectual property.
Results of Sacramento County EBT SCAM Investigation to date

November 2017 through May 2019
- Additional victims located through comparing PIN change data provided by FIS. Thefts were occurring throughout the month, though still heavily concentrated on the first three days.

Locations:
- Started off mostly at ATMs located inside 7-11 stores
- Began also using Citibank and Chase locations in February & March 2018, heavy use started in September 2018. Locations discovered included:
  - 35 7-11 Stores
  - 31 Chase Bank locations
  - 7 Citibank locations
  - 7 stand-alone ATM locations
Investigation Results continued

- **Counties:**
  - 31 counties had victims (Ventura Co. also had one “attempted” victim)

- **Victims:**
  - There were 1,687 individuals whose cards were compromised and withdrawals attempted
  - A total of 1,647 victims who suffered a loss – some of these victims were hit multiple times

- **Loss:**
  - To date, we have found 2,211 completed EBT transactions
  - Loss of $878,646 loss
The question of $949,532.55

What are all the sources of the money? (Not all of it is EBT fraud.)

What about crypto currency?
  - Discovered Crypto wallet with 0.5 BTC

What portion of the recovered money can be used for restitution for EBT theft victims?
EBT Theft Reimbursement Gap

- There were far more potential victims than claims for reimbursement. Why?
- Client misunderstanding. Historically, the official policy of California was not to reimburse theft when the client shared their PIN with an outsider (even if by trickery). This changed in January 2019, but clients may not be aware that they are eligible for reimbursement.
- Lag in filing claims.
- An indication that the client may not be in need of benefits.
- CDSS will partner with counties and stakeholders to develop an outreach strategy.
Identifying Third Party EBT Fraud

• EBT data can help identify and confirm third party fraud.
• **Locational element.** Withdrawal is many miles away from client address, place of work, or previous transaction activity
• **Timing element.** Withdrawal occurs just after benefit issuance.
• PIN change less than 24 hours before withdrawal.
• None of the above prove third-party fraud, but when combined with a statement signed under penalty of perjury by the cardholder, the above elements present a highly likely scenario of third party fraud.
Potential Solutions

• Activating card verification value (CVV) on EBT cards. It’s the 3 digit code on the back of typical debit and credit cards.

• Client education about better guarding their PINs (messaging, posters, flyers, bulletins, etc.)

• Examine call center security and internal controls

• Altering the PIN reset process/ password authentication

• Other “friction” such as limiting PIN changes or withdrawal times
Activating CVV—Implementation Considerations

Advantages

• The CVV code is embedded in the FIS EBT cards, even though the number is not printed on the card.

• Specifically, CVV is embedded in the Trac II data in the magnetic stripe.

• Very effective countermeasure against scamming. A scammer cannot obtain the CVV code through trickery because the cardholder does not know the code.

• Once cardholders possess and activate a modern FIS card, no change in cardholder functionality
Issues/Concerns

• Requires massive card replacement because only 400,000 of California’s 3 million active EBT cards are modern FIS cards. (CA did not mass replace during cutover to FIS in 2018.)

• Implementing CVV will impact cardholder transactions at non-compliant retailers/ATMs which do not send the complete Track II data

• Preliminary data analysis by OSI and FIS suggests that between 1 percent and 9 percent of transactions could be disrupted if CVV were activated now.

• Outreach to retail and financial entities to modernize their systems should reduce the potential for transaction disruption

• Need for cardholder and stakeholder outreach and buy-in

• Activating CVV does not address the threat of skimming.

• What to do about keying card numbers when card not functioning?
Policy Issues

• Better communication among federal, state and local partners.

• State where funds are being withdrawn may be different than the state issuing the benefits. Information tends to develop and stay in the benefit issuing state.

• Develop/collaborate on best practices for preventing third party fraud.

• Benefit replacement policy for EBT cardholders who have had TANF or SNAP benefits stolen by third parties? State versus federal?

• Making Trac II data transmittal a more formal retailer requirement.
Questions?
Contact Information

Todd Bland, Assistant Director
California Department of Social Services
Automation, Integrity and Client Initiatives Branch
744 P Street
Sacramento, CA 95814
Main office line (my assistant): 916-654-2125